GSNA$^{\text{Q\&As}}$

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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 2

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You are concerned about the vulnerabilities existing in the network of the company.

Which of the following can be a cause for making the network vulnerable? (Choose two)

A. Use of well-known code

B. Use of uncommon code

C. Use of uncommon software

D. Use of more physical connections

Correct Answer: AD

In computer security, the term vulnerability is a weakness which allows an attacker to reduce a system\\'s Information Assurance. A computer or a network can be vulnerable due to the following reasons:

Complexity: Large, complex systems increase the probability of flaws and unintended access points. Familiarity: Using common, well-known code, software, operating systems, and/or hardware increases the probability an attacker has or can

find the knowledge and tools to exploit the flaw. Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability.

Password management flaws: The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re- use passwords between

many programs and websites.

Fundamental operating system design flaws: The operating system designer chooses to enforce sub optimal policies on user/program management. For example, operating systems with policies such as default permit grant every program

and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator. Internet Website Browsing: Some Internet websites may contain harmful Spyware

or Adware that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals. Software bugs:

The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.

Unchecked user input: The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-

validated inputs).

Answers B, C are incorrect. Use of common software and common code can make a network vulnerable.

QUESTION 3

Samantha works as a Web Developer for XYZ CORP. She is designing a Web site for the company. In a Web page, she uses the HTTP-EQUIV attribute to control the page cache. Which of the following HTTP-EQUIV values controls the page cache in the browser folder?

A. Window-target

B. Status-code

C. Content-type

D. Pragma

Correct Answer: D

HTTP-EQUIV is an attribute of the META tag. It sets or retrieves information used to bind the META tag\\'s content to an HTTP response header. The pragma value of HTTP-EQUIV controls the page cache.

QUESTION 4

A sequence number is a 32-bit number ranging from 1 to 4,294,967,295. When data is sent over the network, it is broken into fragments (packets) at the source and reassembled at the destination system. Each packet contains a sequence number that is used by the destination system to reassemble the data packets in the correct order. The Initial Sequence Number of your computer is 24171311 at login time. You connect your computer to a computer having the IP address

210.213.23.21. This whole process takes three seconds.

What will the value of the Initial Sequence Number be at this moment?

A. 24171811

B. 24619311

C. 24171111

D. 24171311

Correct Answer: B

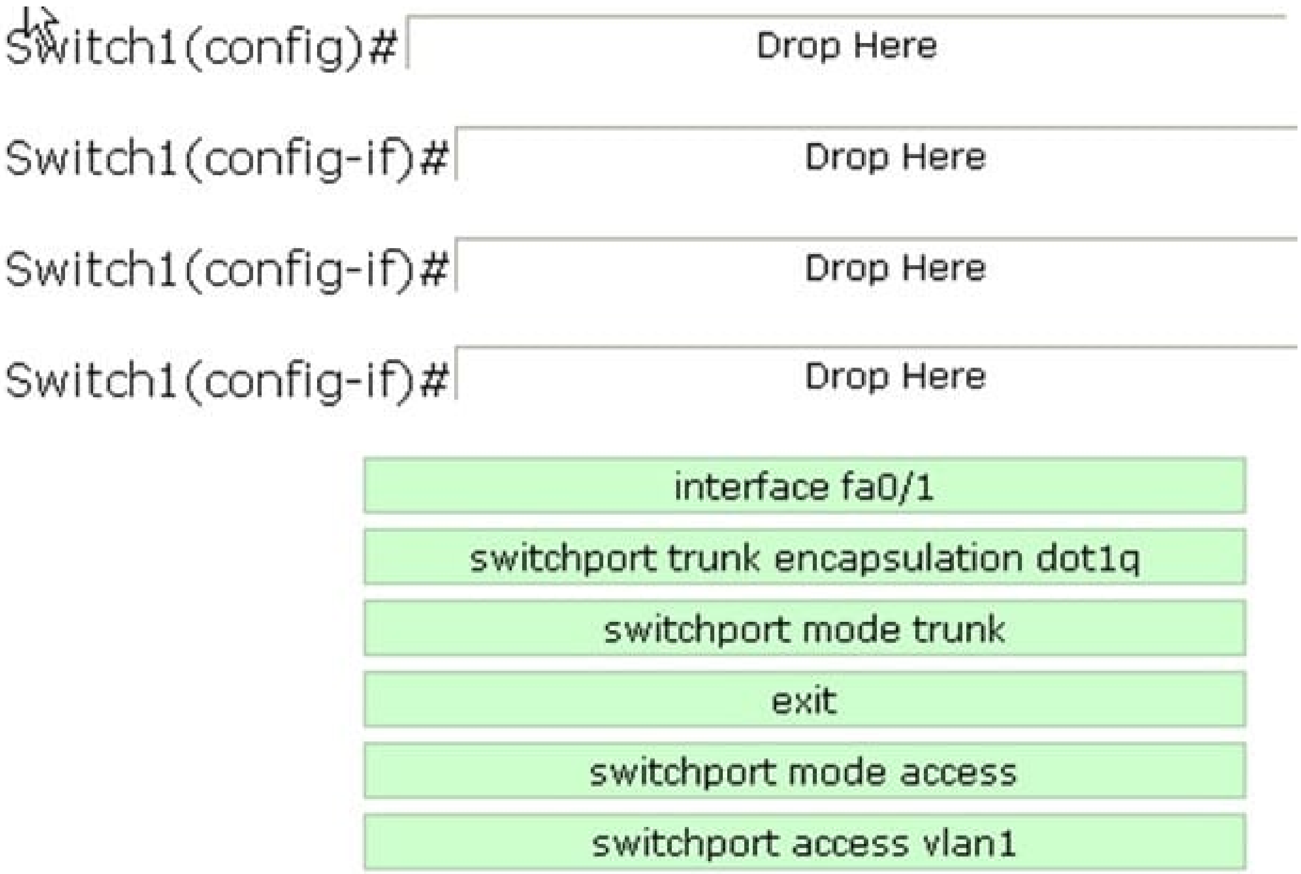
You took 3 seconds to establish a connection. During this time, the value of the Initial Sequence Number would become [24171311 + (1 * 64000) + (3 * 128000)], i.e., 24619311.

QUESTION 5

DRAG DROP

You have created VLANs in your network and have assigned interfaces to each VLAN. You want to configure trunking for carrying traffic of VLANs over a point-to-point link between a switch and a wireless LAN controller. Drag and drop the appropriate commands beside their respective command prompts.

Select and Place:



Switch1(config)# Drop Here

Switch1(config-if)# Drop Here

Switch1(config-if)# Drop Here

Switch1(config-if)# Drop Here

interface fa0/1

switchport trunk encapsulation dot1q

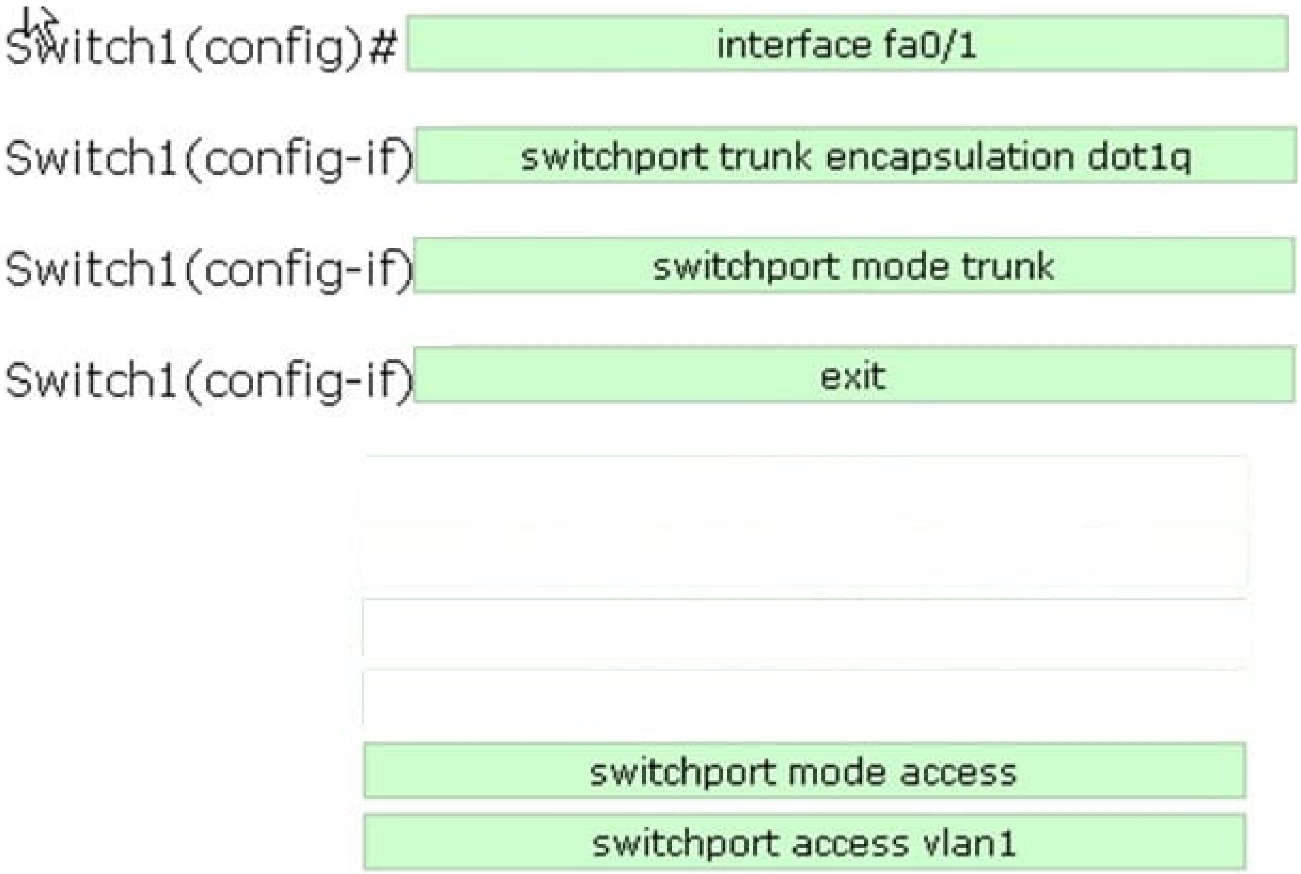
switchport mode trunk

exit

switchport mode access

switchport access vlan1

Correct Answer:



```
Switch1(config)#     interface fa0/1
Switch1(config-if)   switchport trunk encapsulation dot1q
Switch1(config-if)   switchport mode trunk
Switch1(config-if)   exit

                     switchport mode access
                     switchport access vlan1
```

Between an access point and a wireless LAN controller, you will have to execute the following commands in command-line mode: Switch1(config)#interface fa0/1 Switch1(config-if)#switchport trunk encapsulation dot1q Switch1(config-if)#switchport mode trunk Switch1(config-if)#exit You will have to use the interface fa slot/port global configuration command to select a specific Fast Ethernet interface that you want to configure. The switchport trunk encapsulation dot1q command is used to define a trunking protocol as 802.1Q. The switchport mode trunk command is used to define an interface as a trunk.

The exit command is used to return to the previous mode.

QUESTION 6

Which of the following mechanisms is closely related to authorization?

A. Sending secret data such as credit card information.

B. Allowing access to a particular resource.

C. Verifying username and password.

D. Sending data so that no one can alter it on the way.

Correct Answer: B

Authorization is a process that verifies whether a user has permission to access a Web resource. A Web server can restrict access to some of its resources to only those clients that log in using a recognized username and password. To be authorized, a user must first be authenticated. Answer: C is incorrect. Verifying username and password describes the mechanism of authentication. Authentication is the process of verifying the identity of a user. This is usually done using a

user name and password. This process compares the provided user name and password with those stored in the database of an authentication server.

Answer: D is incorrect. Sending data so that no one can alter it on the way describes the mechanism of data integrity. Data integrity is a mechanism that ensures that the data is not modified during transmission from source to destination.

This means that the data received at the destination should be exactly the same as that sent from the source.

Answer: A is incorrect. Sending secret data such as credit card information describes the mechanism of confidentiality. Confidentiality is a mechanism that ensures that only the intended, Authorized recipients are able to read data. The data is

so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.

QUESTION 7

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools?

A. Snort

B. IDS

C. Firewall

D. WIPS

Correct Answer: D

Wireless intrusion prevention system (WIPS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices. Rogue devices can spoof MAC address of an authorized network device as their own. WIPS uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices. Answer B is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components:

1.

Sensors

2.

Console

3.

Engine

Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations,

these three components are combined into a single device.

Basically, following two types of IDS are used:

1.

Network-based IDS

2.

Host-based IDS

Answer: A is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed

for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as

follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console.

Packet logger mode: It logs the packets to the disk.

Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer: C is incorrect. A firewall is a tool to provide security to a

network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the

Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports.

QUESTION 8

You work as a Web Developer for XYZ CORP. The company has a Windows-based network. You have been assigned the task to secure the website of the company. To accomplish the task, you want to use a website monitoring service.

What are the tasks performed by a website monitoring service?

A. It checks the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network.

B. It checks SSL Certificate Expiry.

C. It checks HTTP pages.

D. It checks Domain Name Expiry.

Correct Answer: BCD

Website monitoring service can check HTTP pages, HTTPS, FTP, SMTP, POP3, IMAP, DNS, SSH, Telnet, SSL, TCP, PING, Domain Name Expiry, SSL Certificate Expiry, and a range of other ports with great variety of check intervals from every four hours to every one minute. Typically, most website monitoring services test a server anywhere between once-per hour to once-per-minute. Advanced services offer in-browser web transaction monitoring based on browser add-ons such as Selenium or iMacros. These services test a website by remotely controlling a large number of web browsers. Hence, it can also detect website issues such a JavaScript bugs that are browser specific. Answer: A is incorrect. This task is performed under network monitoring. Network tomography deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet.

QUESTION 9

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 perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party.

Which of the following scanning techniques will John use to accomplish his task?

A. UDP

B. RPC

C. IDLE

D. TCP SYN/ACK

Correct Answer: C

The IDLE scan is initiated with the IP address of a third party. Hence, it becomes a stealth scan. Since the IDLE scan uses the IP address of a third party, it becomes quite impossible to detect the hacker. Answer: B is incorrect. The RPC (Remote Procedure Call) scan is used to find the RPC applications. After getting the RPC application port with the help of another port scanner, RPC port scanner sends a null RPC packet to all the RPC service ports, which are open into the target system. Answer: A is incorrect. In UDP port scanning, a UDP packet is sent to each port of the target system. If the remote port is closed, the server replies that the remote port is unreachable. If the remote Port is open, no such error is generated. Many firewalls block the TCP port scanning, at that time the UDP port scanning maybe useful. Certain IDS and firewalls can detect UDP port scanning easily. Answer: D is incorrect. TCP SYN scanning is also known as half-open scanning because in this a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:

1.The attacker sends SYN packet to the target port.

2.

If the port is open, the attacker receives SYN/ACK message.

3.

Now the attacker breaks the connection by sending an RST packet.

4.

If the RST packet is received, it indicates that the port is closed. This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

1.

It is Linux-based WLAN WEP cracking tool that recovers encryption keys.

2.

It operates by passively monitoring transmissions.

3.

It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

A. Cain

B. PsPasswd

C. Kismet

D. AirSnort

Correct Answer: D

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 the

WEP keys.

Answer: C is incorrect. Kismet is an IEEE 802.11 wireless network sniffer and intrusion detection system.

QUESTION 11

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set some terminal characteristics and environment variables.

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

A. /etc/sysconfig/routed

B. /proc/net

C. /etc/sysconfig/network-scripts/ifcfg-interface

D. /etc/sysconfig/init

Correct Answer: D

In Unix, the /etc/sysconfig/init file is used to set terminal characteristics and environment variables. Answer: B is incorrect. In Unix, the /proc/net file contains status information about the network protocols. Answer: C is incorrect. In Unix, the /

etc/sysconfig/network-scripts/ifcfg-interface file is the configuration file used to define a network interface.

Answer: A is incorrect. In Unix, the /etc/sysconfig/routed file is used to set up the dynamic routing policies.

QUESTION 12

Which of the following backup sites takes the longest recovery time?

A. Mobile backup site

B. Warm site

C. Cold site

D. Hot site

Correct Answer: C

A cold backup site takes the longest recovery time. It is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster. Answer: D is incorrect. A hot site is a duplicate of the original site of the organization, with full computer systems as well as near- complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Ideally, a hot site will be up and running within a matter of hours or even less. Answer: A is incorrect. Although a mobile backup site provides rapid recovery, it does not provide full recovery in time. Hence, a hot site takes the shortest recovery time. Answer: B is incorrect. A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

QUESTION 13

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to do RARP mapping from hardware mapping addresses to IP addresses.

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

A. /etc/dhcpd.conf

B. /etc/motd

C. /etc/exports

D. /etc/ethers

Correct Answer: D

In Unix, the/etc/ethers file is used by system administrators for RARP mapping from hardware mapping addresses to IP addresses.

Answer: A is incorrect. In Unix, the /etc/dhcpd.conf file is the configuration file for the DHCP server daemon.

Answer: C is incorrect. In Unix, the /etc/exports file describes exported file systems for NFS services. Answer: B is incorrect. In Unix, the /etc/motd file automatically displays the message of the day after a successful login.

QUESTION 14

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? (Choose two)

A. TLS

B. SSL

C. HTTP

D. SNMP

Correct Answer: AB

SSL and TLS protocols are used to provide secure communication between a client and a server over the Internet.

QUESTION 15

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.

Latest GSNA Dumps GSNA VCE Dumps GSNA Practice Test