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

In which of the following attacking methods does an attacker distribute incorrect IP address?

A. DNS poisoning

B. IPspoofing

C. Mac flooding

D. Man-in-the-middle

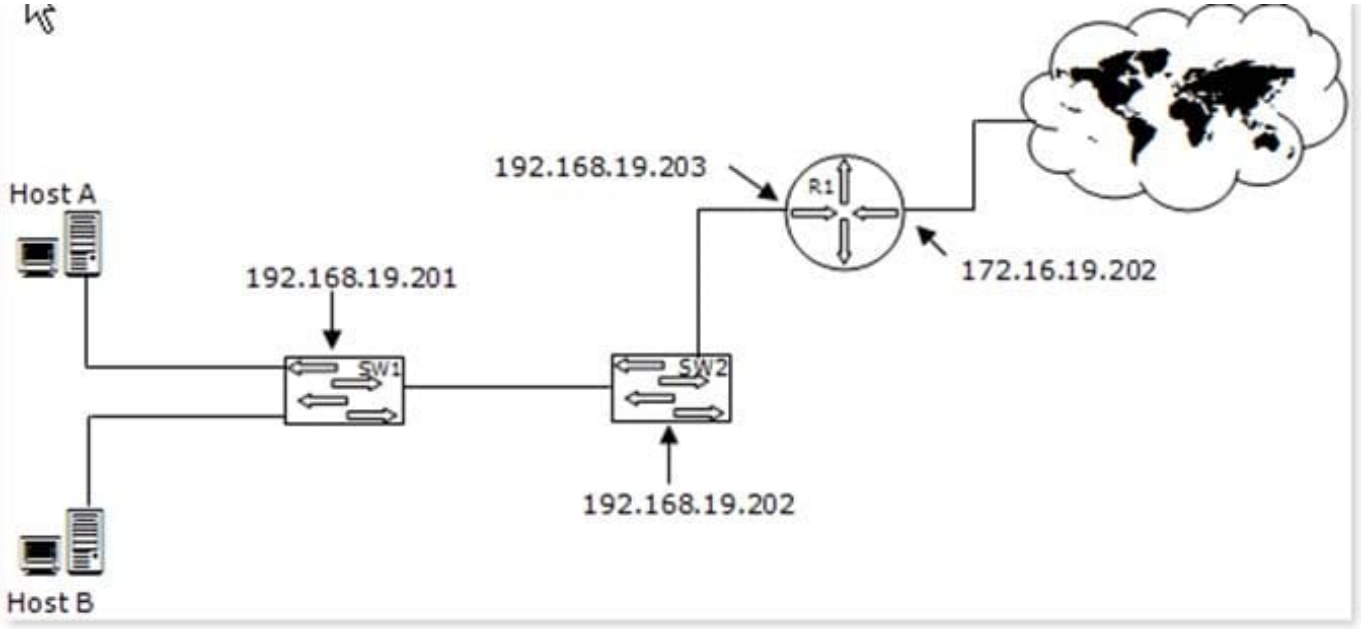
Correct Answer: A

In DNS poisoning attack, an attacker distributes incorrect IP address. DNS cache poisoning is a maliciously created or unintended situation that provides data to a caching name server that did not originate from authoritative Domain Name System (DNS) sources. Once a DNS server has received such non-authentic data, Caches it for future performance increase, it is considered poisoned, supplying the non-authentic data to the clients of the server. To perform a cache poisoning attack, the attacker exploits a flaw in the DNS software. If the server does not correctly validate DNS responses to ensure that they are from an authoritative source, the server will end up caching the incorrect entries locally and serve them to other users that make the same request. Answer: B is incorrect. IP (Internet Protocol) address spoofing is an attack in which an attacker creates the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system. The basic protocol for sending data over the Internet and many other computer networks is the Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response. Answer: D is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer: C is incorrect. MAC flooding is a technique employed to compromise the security of network switches. In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memoryset aside in the switch to store the MAC address-to-physical port translation table. The result of this attack causes the switch to enter a state called fail open mode, in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation. A malicious user could then use a packet sniffer (such as Wireshark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and instant messaging conversations), which would not be accessible were the switch operating normally.

QUESTION 2

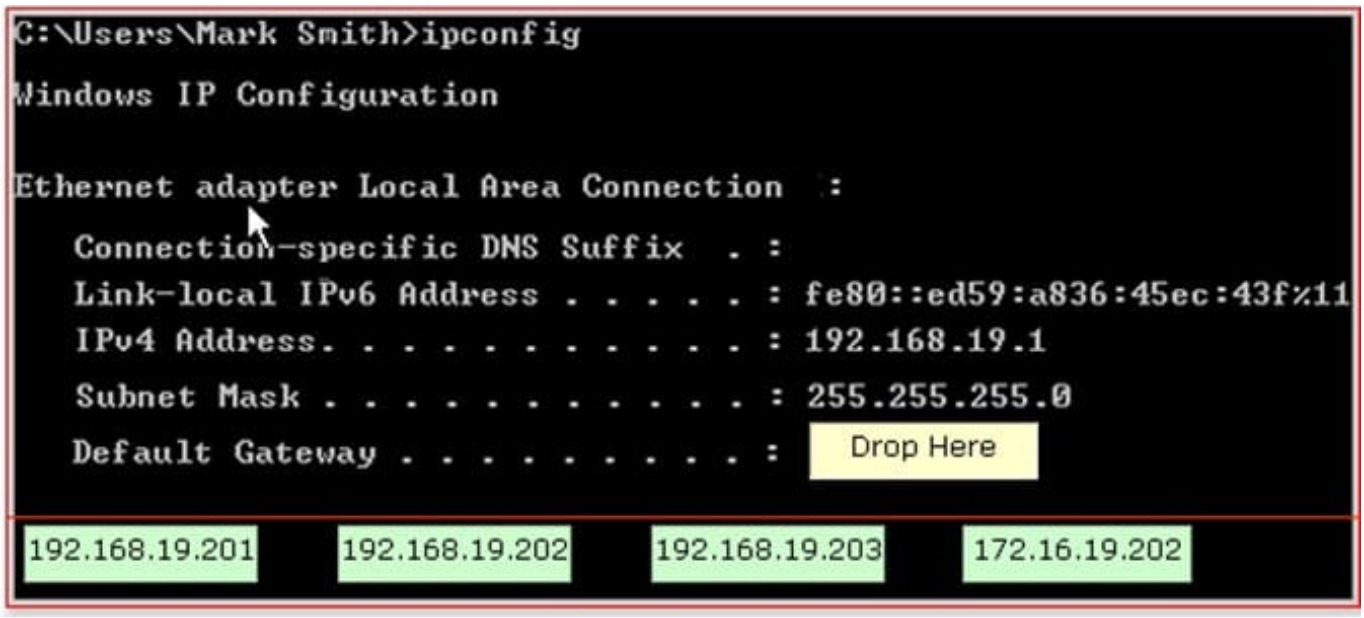
DRAG DROP

You work as a Network Administrator for Blue Well Inc. The company has a TCP/IP-based network environment. The network contains Cisco switches and a Cisco Catalyst router. The network is configured as shown in the image below:

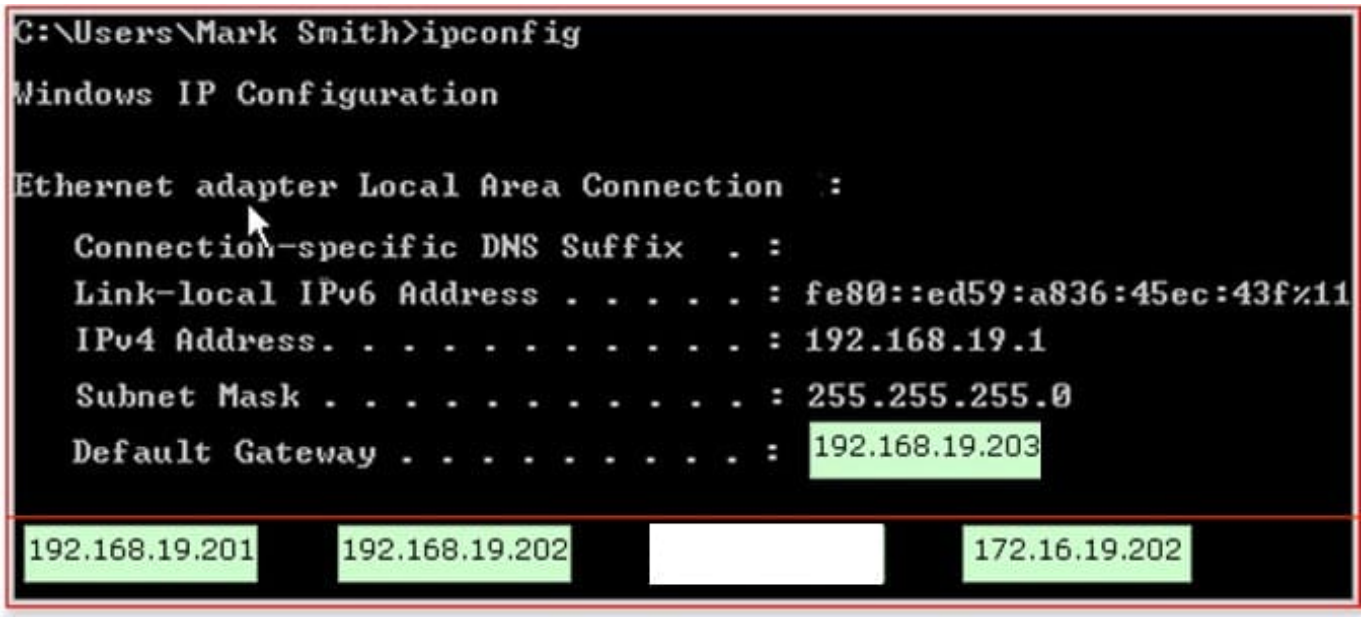


You want to enable Host A to access the Internet. For this, you need to configure the default gateway settings. Choose the appropriate address to accomplish the task.

Select and Place:



Correct Answer:



According to the question, you are required to configure the default gateway setting on Host A so that users can access the Internet through it. For a computer to communicate with computers on another segment in a routed network, it is important to configure the default gateway. In order to accomplish the task, you will have to set the address 192.168.19.203 as the default gateway address.

QUESTION 3

You are the Security Consultant and have been hired to check security for a client\\'s network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server.

What should be your highest priority then in checking his network?

A. Setting up a honey pot

B. Vulnerability scanning

C. Setting up IDS

D. Port scanning

Correct Answer: B

According to the question, you highest priority is to scan the Web applications for vulnerability.

QUESTION 4

Which of the following processes is described in the statement below?

"This is the process of numerically analyzing the effect of identified risks on overall project objectives."

A. Perform Quantitative Risk Analysis

B. Monitor and Control Risks

C. Perform Qualitative Risk Analysis

D. Identify Risks

Correct Answer: A

Perform Quantitative Risk Analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. This process generally follows the Perform Qualitative Risk Analysis process. It is performed on risks that have been prioritized by the Perform Qualitative Risk Analysis process as potentially and substantially impacting the project\\'s competing demands. The Perform Quantitative Risk Analysis should be repeated after Plan Risk Responses, as well as part of Monitor and Control Risks, to determine if the overall project risk has been decreased. Answer: C is incorrect. This is the process of prioritizing risks for further analysis or action by accessing and combining their probability of occurrence and impact. Answer: D is incorrect. This is the process of determining which risks may affect the project and documenting their characteristics. Answer: B is incorrect. This is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness through the project.

QUESTION 5

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP based switched network. A root bridge has been elected in the switched network. You have installed a new switch with a lower bridge ID than the existing root bridge.

What will happen?

A. The new switch starts advertising itself as the rootbridge.

B. The new switch divides the network into two broadcast domains.

C. The new switch works as DR or BDR.

D. The new switch blocks all advertisements.

Correct Answer: A

The new switch starts advertising itself as the root bridge. It acts as it is the only bridge on the network. It has a lower Bridge ID than the existing root, so it is elected as the root bridge after the BPDUs converge and when all switches know

about the new switch that it is the better choice.

Answer: B, C, D are incorrect. All these are not valid options, according to the given scenario.