Free Questions for GSNA by certscare

Shared by Hart on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You work as a programmer for uCertify.Inc. You have a session object named session1 with an attribute named Attribute1, and an HttpSessionBindingEvent object binding1 bound to session1. Which of the following will be used to retrieve Attribute1?

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

Options:

A- Object obj=binding1.getSession().getAttribute('Attribute1');

B- Object obj=binding1.getAttribute('Attribute1');

C- Long MyAttribute=session1.getAttribute('Attribute1');

D- Object obj=session1.getAttribute('Attribute1');

E- String str1=session1.getAttribute('Attribute1');

Answer:

A, D

Explanation:

The following two code are used to retrieve Attribute1:

1.Object obj=session1.getAttribute('Attribute1'); The getAttribute() method is used to retrieve the bound object with the specified name in this session, or null if no object is bound under the name.

2.Object obj=binding1.getSession().getAttribute('Attribute1'); The getSession() gets the current valid session associated with this request.

Answer E and C are incorrect. These code are invalid because the getAttribute() method returns an object instead of a long object or a String object.

Answer B is incorrect. The HttpSessionBindingEvent object cannot use the getAttribute() method.

Question 2

Question Type: **MultipleChoice**

Web applications are accessed by communicating over TCP ports via an IP address. Choose the two most common Web Application TCP ports and their respective protocol names.

Each correct answer represents a complete solution. Choose two.

Options:

A- TCP Port 443 / S-HTTP or SSL

B- TCP Port 80 / HTTPS or SSL

C- TCP Port 443 / HTTPS or SSL

D- TCP Port 80 / HTTP

Answer:

C, D

Explanation:

The two most common Web Application TCP ports are Port 443 and Port 80. HTTPS or SSL uses TCP port 443, whereas HTTP uses TCP Port 80.

Answer B is incorrect. Port 80 is used for HTTP, not HTTPS.

Answer A is incorrect. S-HTTP is not the protocol name for Port 443. HTTPS or SSL is the name used for Port 443 traffic.

Question 3

Question Type: MultipleChoice

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

Options:

A- Incontrovertible

B- Corroborating

C- Direct

D- Circumstantial

Answer:

D

Explanation:

Circumstantial evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person.

Answer B is incorrect. Corroborating evidence is evidence that tends to support a proposition that is already supported by some

evidence.

Answer A is incorrect. Incontrovertible evidence is a colloquial term for evidence introduced to prove a fact that is supposed to be so

conclusive that there can be no other truth as to the matter; evidence so strong, it overpowers contrary evidence, directing a fact-finder to a

specific and certain conclusion.

Answer C is incorrect. Direct evidence is testimony proof for any evidence, which expressly or straight-forwardly proves the existence of

a fact.

Question 4

Question Type: **MultipleChoice**

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

Options:

A- DNS poisoning

B- IP spoofing

C- Mac flooding

D- Man-in-the-middle

Answer:

A

Explanation:

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 and 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 memory set

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 failopen 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 5

Question Type: MultipleChoice

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 break a dat

a.txt file, 200MB in size, into two files in which the size of the first file named data.txt.aa should be 150MB and that of the second file named data.txt.ab should be 50MB. To accomplish his task and to further delete the data.txt file, he enters the following command:

split --verbose -b 150m data.txt data.txt. ; rm -vf data.txt

Which of the following commands can John use to join the splitted files into a new data.txt file?

Options:

A- vi data.txt.* > data.txt

B- less data.txt.* > data.txt

C- vi data.txt.*

D- cat data.txt.* > data.txt

Answer:

D

Explanation:

The cat data.txt.* command will display both the splitted files, and the > command will redirect the output into a new data.txt file.

Question 6

Question Type: MultipleChoice

Which TCP and UDP ports can be used to start a NULL session attack in NT and 2000 operating systems?

Options:

A- 149 and 133

B- 203 and 333

C- 139 and 445

D- 198 and 173

Answer:

C

Explanation:

A null session is an anonymous connection to a freely accessible network share called IPC$ on Windows-based servers. It allows immediate

read and write access with Windows NT/2000 and read-access with Windows XP and 2003.

The command to be inserted at the DOS-prompt is as follows:

net use \\IP address_or_host name\ipc$ '' '/user:'

net use

Port numbers 139 TCP and 445 UDP can be used to start a NULL session attack.

Question 7

Question Type: **MultipleChoice**

ACID (atomicity, consistency, isolation, and durability) is an acronym and mnemonic device for learning and remembering the four primary attributes ensured to any transaction by a transaction manager. Which of the following attributes of ACID confirms that the committed data will be saved by the system such that, even in the event of a failure or system restart, the data will be available in its correct state?

Options:

A- Durability

B- Atomicity

C- Isolation

D- Consistency

Answer:

A

Explanation:

Durability is the attribute of ACID which confirms that the committed data will be saved by the system such that, even in the event of a failure or system restart, the data will be available in its correct state.

Answer B is incorrect. Atomicity is the attribute of ACID which confirms that, in a transaction involving two or more discrete pieces of information, either all of the pieces are committed or none are.

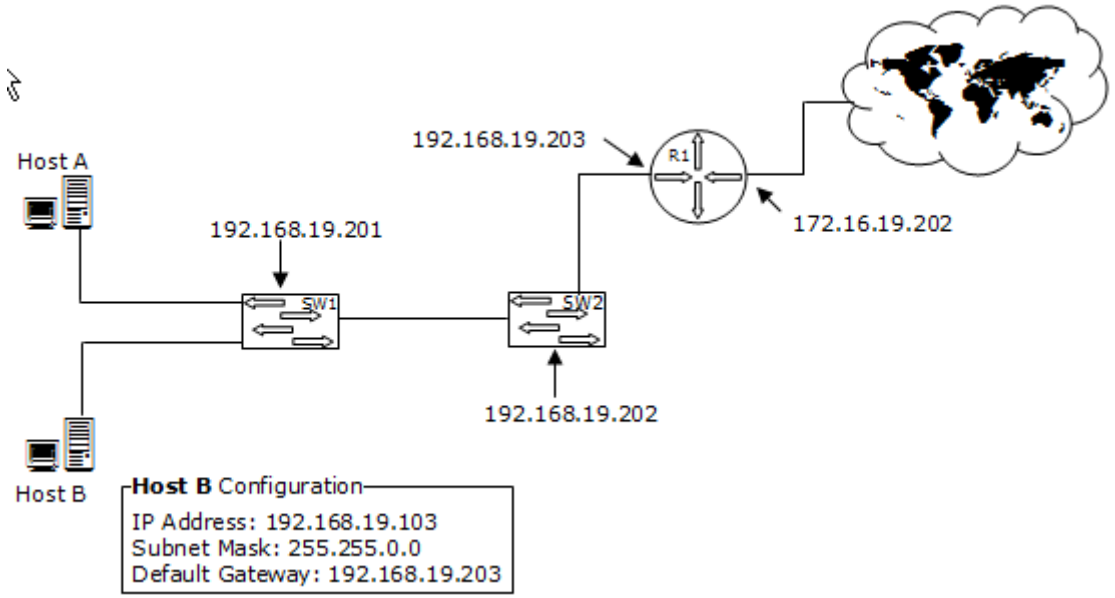
Answer D is incorrect. Consistency is the attribute of ACID which confirms that a transaction either creates a new and valid state of data, or, if any failure occurs, returns all data to its state before the transaction was started.

Answer C is incorrect. Isolation is the attribute of ACID which confirms that a transaction in process and not yet committed must remain isolated from any other transaction.

Question 8

Question Type: MultipleChoice

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP-based network environment. The network contains Cisco switches and a Cisco router. A user is unable to access the Internet from Host B. You also verify that Host B is not able to connect to other resources on the network. The IP configuration of Host B is shown below:



Which of the following is the most likely cause of the issue?

Options:

A- An incorrect subnet mask is configured on Host B.

B- The IP address of Host B is not from the correct IP address range of the network.

C- There is an IP address conflict on the network.

D- An incorrect default gateway is configured on Host B.

Answer:

A

Explanation:

According to the network diagram, the IP address range used on the network is from the class C private address range. The class C IP address uses the following default subnet mask:

255.255.255.0

The question specifies that the subnet mask used in Host B is 255.255.0.0, which is an incorrect subnet mask.

To Get Premium Files for GSNA Visit

https://www.p2pexams.com/products/gsna

For More Free Questions Visit

https://www.p2pexams.com/giac/pdf/gsna