Vendor:GIAC

Exam Code:GCIH

Exam Name:GIAC Certified Incident Handler

Version: Demo

QUESTION 1

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following

actions:

Remove the network cable wires.

Isolate the system on a separate VLAN

Use a firewall or access lists to prevent communication into or out of the system.

Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

A. Identification

B. Containment

C. Eradication

D. Recovery

Correct Answer: B

QUESTION 2

FILL BLANK

Fill in the blank with the appropriate term.

_______is the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

A.

B.

C.

D.

Correct Answer:

QUESTION 3

Which of the following statements about threats are true?

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

A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.

B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.

D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

Correct Answer: BCD

QUESTION 4

Which of the following can be used to perform session hijacking?

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

A. Cross-site scripting

B. Session fixation

C. ARP spoofing

D. Session sidejacking

Correct Answer: ABD

QUESTION 5

Which of the following attacks allows an attacker to retrieve crucial information from a Web server\\'s database?

A. Database retrieval attack

B. PHP injection attack

C. SQL injection attack

D. Server data attack

Correct Answer: C

QUESTION 6

You run the following PHP script:

What is the use of the mysql_real_escape_string() function in the above script. Each correct answer represents a complete solution. (Choose all that apply.)

A. It can be used to mitigate a cross site scripting attack.

B. It can be used as a countermeasure against a SQL injection attack.

C. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except \\' and ".

D. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

Correct Answer: BD

QUESTION 7

An engineer is using Hashcat to brute force passwords from a file of hashes. How should the following hash be handled in the scenario? aad3b435b51404eeaad3b435b51404ee

A. The hash should be skipped

B. The hash should be cracked as a SHA-1 hash

C. The hash should be decoded

D. The hash should be cracked as an NT hash

Correct Answer: B

QUESTION 8

Adam works as a sales manager for Umbrella Inc. He wants to download software from the Internet. As the software comes from a site in his untrusted zone, Adam wants to ensure that the downloaded software has not been Trojaned. Which of the following options would indicate the best course of action for Adam?

A. Compare the file size of the software with the one given on the Website.

B. Compare the version of the software with the one published on the distribution media.

C. Compare the file\\'s virus signature with the one published on the distribution.

D. Compare the file\\'s MD5 signature with the one published on the distribution media.

Correct Answer: D

QUESTION 9

You are in the process of recovering from an incident where a web server and database server were severely compromised due to a lack of patching. Both servers have been rebuilt and fully patched. Which of the following choices BEST describes what you should do next?

A. Recommend that the business owners make sure they keep their systems patched up to date

B. Ask the business owners to test both systems to ensure the necessary functionality is present

C. Tell the business owners that all needed functionality is present

D. Ask the business owners when to put the systems back into production

E. Tell the business owners when you will put the systems back into production

Correct Answer: A

QUESTION 10

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.

Which of the following are the techniques used for network mapping by large organizations?

Each correct answer represents a complete solution. (Choose three.)

A. Packet crafting

B. Route analytics

C. SNMP-based approaches

D. Active Probing

Correct Answer: BCD

QUESTION 11

Adam, a novice web user, is very conscious about the security. He wants to visit the Web site that is known to have malicious applets and code. Adam always makes use of a basic Web Browser to perform such testing.

Which of the following web browsers can adequately fill this purpose?

A. Mozilla Firefox

B. Internet explorer

C. Lynx

D. Safari

Correct Answer: C

QUESTION 12

What is one of the first actions you should take in the containment phase of incident handling?

A. Provide the system administrator with input regarding disconnecting the system from the network, but leave the decision up to them

B. Provide management with incident details so they can decide whether or not to disconnect the system

C. Decide whether to remove the system from the network via a team vote. Be sure to include all involved

D. Leave the system on the network in order to watch the attacker and collect evidence

Correct Answer: B

You may have strong feelings about leaving the system on the network to catch the intruder, or getting it unplugged to contain the incident, but the decision always comes down to management. Be sure to provide them with input for both sides of the argument, but they will make the call.