Free Questions for GSEC by certsinside

Shared by Salas on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following activities would take place during the containment phase?

Options:

A- Disseminating change management documentation regarding the steps taken during incident.

B- Rebuild a virtual server from scratch using the original installation media.

C- Correlating logs from the firewall, PCAPs from an IPS, and syslogs from a server to build a timeline.

D- Creating a binary backup of the system's Infected hard drive for usage in a forensic Investigation.

Answer:

C

Question 2

Question Type: MultipleChoice

What is a characteristic of iOS security?

Options:

A- Most security features are user configurable

B- Less restrictive architecture than macOS

C- Flaw disclosures are sent to the Open Handset Alliance (OHA)

D- Forbids mobile operator (MO) software

Answer:

A

Question 3

Question Type: MultipleChoice

A database is accessed through an application that users must authenticate with, on a host that only accepts connections from a subnet where the business unit that uses the data is located. What defense strategy is this?

Options:

A- Information Centric

B- Threat Modeling

C- Uniform Production

D- Vector Oriented

Answer:

C

Question 4

Question Type: **MultipleChoice**

What is it called when an OSI layer adds a new header to a packet?

Options:

A- Switching

B- Encapsulation

C- fragmentation

D- Routing

Answer:

B

Question 5

Question Type: MultipleChoice

Which services will have listening ports on a hardened Linux log server?

Options:

A- RPC and SMTP

B- TFTP and telnet

C- SSH and syslog

D- HTTP and SFTP

Answer:

C

Question 6

Question Type: MultipleChoice

What must be added to VLANs to improve security?

Options:

A- Network hubs

B- Air gaps

C- Spanning tree interfaces

D- Access control lists

Answer:

D

Question 7

Question Type: MultipleChoice

A security analyst has entered the following rule to detect malicious web traffic:

alert tcp any -> 192.168.1.0/24 SO (msg: Attempted SQL Injection!"; sld:20000O01;)

How can this rule be changed to reduce false positives?

Options:

A- Change the rule to make it apply bi -directional to source and destination

B- Add more detail in the rule to make it more specific to the attack pattern

C- Add an additional rule to apply to destination port 443 as well as 80

D- Make the IP range more general so that it applies to all webservers

Answer:

B

Question 8

Question Type: MultipleChoice

A program has allocated 10 characters of space for user's response on a form. The application does not validate the number of characters that a user can input into the field before accepting the dat

a. Which type of attack Is the application vulnerable to?

Options:

A- On hijacking

B- Buffet overflow

C- Cross site scripting

D- SQL Injection

Answer:

B