GSEC Q&As

GIAC Security Essentials Certification

Pass GIAC GSEC Exam with 100% Guarantee

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

https://www.certbus.com/gsec.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

What does it mean if a protocol such as HTTP is stateless?

A. The client responds to server request and keeps track of the conversation.

B. If a stateless protocol is used it cannot be traced.

C. It means it is unreliable.

D. The server responds to a single request and then forgets about it.

Correct Answer: D

QUESTION 2

Which of the following statements best describes where a border router is normally placed?

A. Between your firewall and your internal network

B. Between your firewall and DNS server

C. Between your ISP and DNS server

D. Between your ISP and your external firewall

Correct Answer: D

QUESTION 3

Which Host-based IDS (HIDS) method of log monitoring utilizes a list of keywords or phrases that define the events of interest for the analyst, then takes a list of keywords to watch for and generates alerts when it sees matches in log file activity?

A. Passive analysis

B. Retroactive analysis

C. Exclusive analysis

D. Inclusive analysis

Correct Answer: D

QUESTION 4

The following three steps belong to the chain of custody for federal rules of evidence. What additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.

B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.

C. Take photographs of all persons who have had access to the computer.

D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.

Correct Answer: D

QUESTION 5

What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

A. Trojans

B. Boot infectors

C. Viruses

D. Worms

Correct Answer: D

QUESTION 6

Which of the following proxy servers provides administrative controls over the content?

A. Content filtering web proxy server

B. Caching proxy server

C. Forced proxy server

D. Web proxy server

Correct Answer: A

QUESTION 7

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

A. ROI = (gain - expenditure)/(expenditure) X 100%

B. ROI = (gain + expenditure)/(expenditure) X 100%

C. ROI = (loss + expenditure)/(expenditure) X 100%

D. ROI = (loss - expenditure)/(expenditure) X 100%

Correct Answer: A

QUESTION 8

You have implemented a firewall on the company\\'s network for blocking unauthorized network connections. Which of the following types of security control is implemented in this case?

A. Detective

B. Preventive

C. Directive

D. Corrective

Correct Answer: B

QUESTION 9

What is the main reason that DES is faster than RSA?

A. DES is less secure.

B. DES is implemented in hardware and RSA is implemented in software.

C. Asymmetric cryptography is generally much faster than symmetric.

D. Symmetric cryptography is generally much faster than asymmetric.

Correct Answer: D

QUESTION 10

You are implementing wireless access at a defense contractor. Specifications say, you must implement the AES Encryption algorithm. Which encryption standard should you choose?

A. WPA

B. TKIP

C. WEP

D. WPA 2

Correct Answer: D

QUESTION 11

The TTL can be found in which protocol header?

A. UDP

B. TCP

C. IP

D. ICMP

Correct Answer: C

QUESTION 12

Which of the following is a type of countermeasure that can be deployed to ensure that a threat vector does not meet a vulnerability?

A. Prevention controls

B. Detection controls

C. Monitoring controls

D. Subversive controls

Correct Answer: A

QUESTION 13

Where could you go in Windows XP/2003 to configure Automatic Updates?

A. Right click on the Start Menu and choose select Properties in the pop-up Menu.

B. Open the MMC and choose the Automatic Updates snap-in.

C. Right click on your desktop and choose the automatic updates.

D. Go to the System applet in Control Panel and click on the Automatic Updates icon.

Correct Answer: D

QUESTION 14

In trace route results, what is the significance of an * result?

A. A listening port was identified.

B. A reply was returned in less than a second.

C. The target host was successfully reached.

D. No reply was received for a particular hop.

Correct Answer: D

QUESTION 15

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

A. SSL

B. HTTP

C. TLS

D. SNMP

Correct Answer: AC