GCIH$^{\text{Q\&As}}$

GIAC Certified Incident Handler

QUESTION 1

Which of the following functions in c/c++ can be the cause of buffer overflow? Each correct answer represents a complete solution. (Choose two.)

A. printf()

B. strcat()

C. strcpy()

D. strlength()

Correct Answer: BC

QUESTION 2

How does an attacking host initiate a SYN flood attack?

A. It sends many SYN-ACK packets to a target machine from a spoofed address

B. It sends many SYN packets to a target machine from a spoofed address

C. It sends many SYN-RST packets to a target machine from a spoofed address

D. It sends many SYN-FIN packets to a target machine from a spoofed address

Correct Answer: B

Explanation: When a client and server establish a normal TCP "three-way handshake," the exchange looks like this:

1.

Client requests connection by sending SYN (synchronize) message to the server.

2.

Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.

3.

Client responds with an ACK (acknowledge) message, and the connection is established.

QUESTION 3

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denialof-service, or unauthorized changes to system hardware, software, or data?

A. Disaster Recovery Plan

B. Cyber Incident Response Plan

C. Crisis Communication Plan

D. Occupant Emergency Plan

Correct Answer: B

QUESTION 4

Which of the following is one of the fields that Covert TCP uses to transmit data?

A. IP Options

B. Urgent Pointer

C. IP Identification

D. Code Bits

Correct Answer: A

QUESTION 5

Jane works as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. Jane is troubleshooting the computer of a user who has installed software that automatically gains full permissions on his computer. Jane has never seen this software before. Which of the following types of malware is the user facing on his computer?

A. Rootkits

B. Viruses

C. Spyware

D. Adware

Correct Answer: A