GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.geekcert.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

A. Tripwire

B. SubSeven

C. Netstat

D. Fport

Correct Answer: D

QUESTION 2

Which of the following statements are true about netcat?

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

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.

B. It can be used as a file transfer solution.

C. It provides outbound and inbound connections for TCP and UDP ports.

D. The nc -z command can be used to redirect stdin/stdout from a program.

Correct Answer: ABC

QUESTION 3

Which is a requirement to ensure the success of the following command? C:\> notepad helloworld.txt:goodbye.txt

A. Replace "notepad" with "more"

B. Encryption must be disabled on the drive

C. An NTFS partition

D. Installation of a 3rd party tool

Correct Answer: C

The given command shows an alternate data stream being added to the helloworld.txt file. File streaming is supported on NTFS, which allows alternative data streams to be associated with a file; the alternate (read: secondary and thereafter) stream(s) are hidden from view when viewing files normally via Windows Explorer or the command line.

QUESTION 4

Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase

B. Pre-attack phase

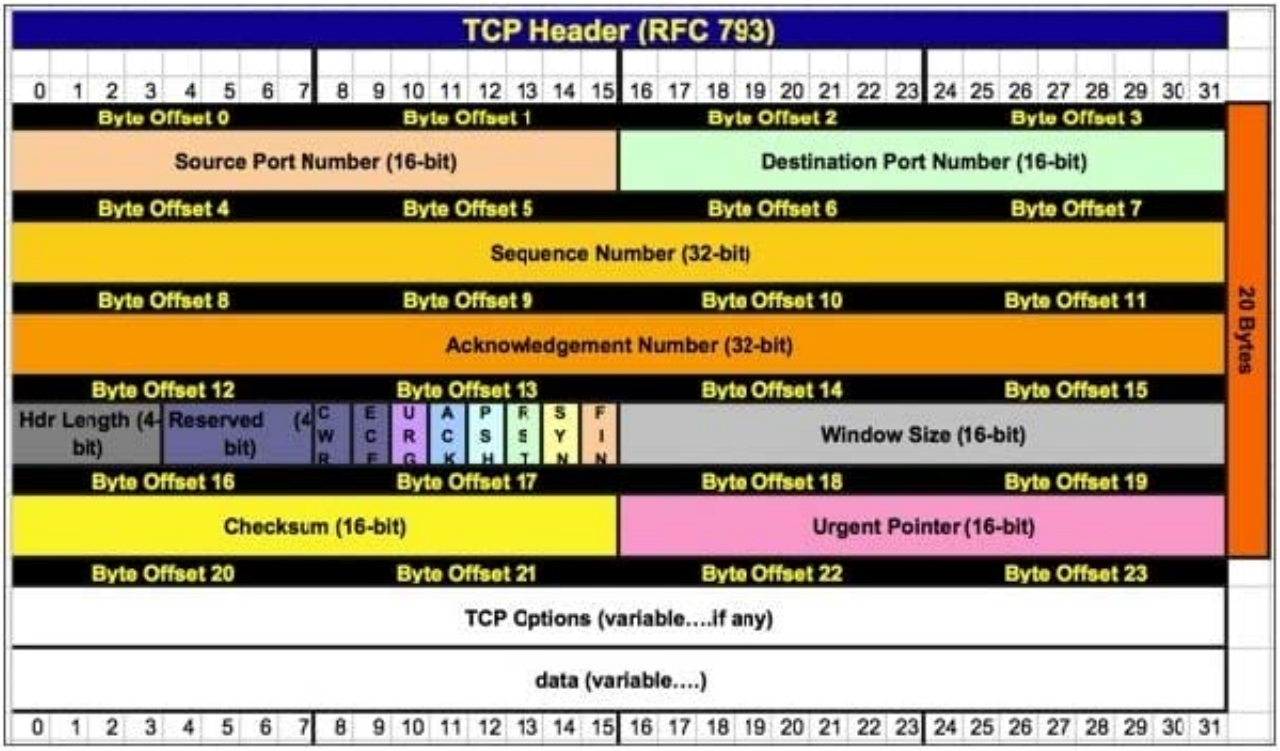
C. Post-attack phase

D. Out-attack phase

Correct Answer: B

QUESTION 5

Covert_TCP will use which of the following byte offsets on the TCP header to carry ASCII data?



A. Byte offset 8-11

B. Byte offset 20-23

C. Byte offset 14 and 15

D. Byte offset 18 and 19

Correct Answer: A

Covert_TCP allows for transmitting information by entering ASCII data in the following TCP header fields:

-TCP initial sequence number

-TCP acknowledgement sequence number

The image reveals that these fields are in Byte offsets 4-7 and 8-11.