312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

A. MD4

B. DES

C. SHA

D. SSL

Correct Answer: B

The LM hash is computed as follows.1. The user\\'s password as an OEM string is converted to uppercase. 2. This password is either null-padded or truncated to 14 bytes. 3. The "fixed-length" password is split into two 7-byte halves. 4. These values are used to create two DES keys, one from each 7-byte half. 5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#$ %", resulting in two 8-byte ciphertext values. 6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

QUESTION 2

In Buffer Overflow exploit, which of the following registers gets overwritten with return address of the exploit code?

A. EIP

B. ESP

C. EAP

D. EEP

Correct Answer: A

EIP is the instruction pointer which is a register, it points to your next command.

QUESTION 3

If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

A. SYN

B. ACK

C. FIN

D. PSH

Correct Answer: AB

The proper response is a SYN / ACK. This technique is also known as half-open scanning.

QUESTION 4

You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000 Server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permission. You need to know what your current privileges are within the shell. Which of the following options would be your current privileges?

A. Administrator

B. IUSR_COMPUTERNAME

C. LOCAL_SYSTEM

D. Whatever account IIS was installed with

Correct Answer: C

If you manage to get the system to start a shell for you, that shell will be running as LOCAL_SYSTEM.

QUESTION 5

John is using a special tool on his Linux platform that has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI/ASPX scripts. Moreover, the database detects DDoS zombies and Trojans as well. What would be the name of this tool?

A. hping2

B. nessus

C. nmap

D. make

Correct Answer: B