GPEN$^{\text{Q\&As}}$

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

QUESTION 1

LM hash is one of the password schemes that Microsoft LAN Manager and Microsoft Windows versions prior to the Windows Vista use to store user passwords that are less than 15 characters long. If you provide a password seven characters or less, the second half of the LM hash is always ___________.

A. 0xBBD3B435B51504FF

B. 0xAAD3B435B51404FF

C. 0xBBC3C435C51504EF

D. 0xAAD3B435B51404EE

Correct Answer: D

QUESTION 2

What problem occurs when executing the following command from within a netcat raw shell? sudo cat /etc/shadow

A. Sudo does not work at all from a shell

B. Sudo works fine if the user and command are both in the /etc/sudoers file

C. The display blanks after typing the sudo command

D. You will not be able to type the password at the password prompt

Correct Answer: A

QUESTION 3

Which of the following statements are true about firewalking?

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

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

B. Firewalking works on the UDP packets.

C. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

Correct Answer: ACD

QUESTION 4

You work as a Web developer in the IBM Inc. Your area of proficiency is PHP. Since you have proper knowledge of security, you have bewared from rainbow attack. For mitigating this attack, you design the PHP code based on the following

algorithm:

```
key = hash(password + salt)

for 1 to 65000 do

key = hash(key + salt)
```

Which of the following techniques are you implementing in the above algorithm?

A. Key strengthening

B. Hashing

C. Sniffing

D. Salting

Correct Answer: A

QUESTION 5

You want to search Microsoft Outlook Web Access Default Portal using Google search on the

Internet so that you can perform the brute force attack and get unauthorized access. What search string will you use to accomplish the task?

A. intitle:index.of inbox dbx

B. intext:"outlook.asp"

C. allinurl:"exchange/logon.asp"

D. intitle:"Index Of" -inurl:maillog maillog size

Correct Answer: C

Latest GPEN Dumps   GPEN Practice Test   GPEN Study Guide