GPEN Q&As

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

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

https://www.passapply.com/gpen.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

You work as an IT Technician for uCertify Inc. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company\\'s wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. MAC Filtering

B. SSID

C. RAS

D. WEP

Correct Answer: A

QUESTION 2

Which of the following describe the benefits to a pass-the-hash attack over traditional password cracking?

A. No triggering of IDS signatures from the attack privileges at the level of theacquired password hash and no corruption of the LSASS process.

B. No triggering of IDS signatures from the attack, no account lockout and use ofnative windows file and print sharing tools on the compromised system.

C. No account lockout, privileges at the level of the acquired password hash and useof native windows file and print Sharif tools on the compromised system.

D. No account lockout, use of native file and print sharing tools on the compromisedsystem and no corruption of the LSASS process.

Correct Answer: D

QUESTION 3

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends large number of unsolicited commercial e-mail (UCE) messages on these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail Spam

B. E-mail Storm

C. E-mail spoofing

D. E-mail bombing

Correct Answer: A

QUESTION 4

A customer has asked for a scan or vulnerable SSH servers. What is the penetration tester attempting to accomplish using the following Nmap command?

```
# nmap -n -sV --script=sshv1.nse 10.10.10.60 -p 22
```

A. Checking operating system version

B. Running an exploit against the target

C. Checking configuration

D. Checking protocol version

Correct Answer: D

QUESTION 5

What command will correctly reformat the Unix passwordcopy and shadowcopy Tiles for input to John The Ripper?

A. /un shadow passwd copy shadowcopy > johnfile

B. /unshadow passwdcopy shadowcopy > johnfile

C. /unshadow shadowcopy passwdcopy >john file

D. /unshadow passwdcopy shadowcopy > johnfile

Correct Answer: B