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

How can a non-privileged user on a Unix system determine if shadow passwords are being used?

A. Read /etc/password and look for "x" or "II" in the second colon-delimited field

B. Read /etc/shadow and look for "x" or "II" in the second colon-delimited field

C. Verify that /etc/password has been replaced with /etc/shadow

D. Read /etc/shadow and look NULL values In the second comma delimited field

Correct Answer: B

QUESTION 2

Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. snort_inline

B. EtherApe

C. Snort decoder

D. AirSnort

Correct Answer: C

QUESTION 3

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement WPA

C. Don\\'t broadcast SSID

D. Implement MAC filtering

Correct Answer: C

QUESTION 4

Analyze the excerpt from a packet capture between the hosts 192.168.116.9 and 192.168.116.101. What factual conclusion can the tester draw from this output?

```
19:18:01.943630 IP 192.168.116.9.36155 > 192.168.116.101.135: S 3470088794:3470088794
(0) win
19:18:01.944019 IP 192.168.116.9.53541 > 192.168.116.101.139: S 3468017513:3468017513
(0) win 5840 <mss 1460,sackOK,timestamp 1133348468 0,nop,wscale 5>
19:18:01.944903 IP 192.168.116.101.139 > 192.168.116.9.53541: S 627552668:627552668(0)
ack 3468017514 win 65535 <mss 1460,nop,wscale 0,nop,nop,timestamp 0,nop,nop,sackOK>
19:18:01.944925 IP 192.168.116.9.53541 > 192.168.116.101.139: . ack 1 win 183
<nop,nop,timestamp 1133348468 0>
19:18:01.945122 IP 192.168.116.9.53541 > 192.168.116.101.139: R 1:1(0) ack 1 win 183
<nop,nop,timestamp 1133348468 0>
```

A. Port 135 is filtered, port 139 is open.

B. Pons 135 and 139 are filtered.

C. Ports 139 and 135 are open.

D. Port 139 is closed, port 135 is open

Correct Answer: C

QUESTION 5

Why is it important to have a cheat sheet reference of database system tables when performing SQL Injection?

A. This is where sites typically store sensitive information such as credit card numbers.

B. These tables contain a list of allowed database applications

C. The information in these tables will reveal details about the web application\\'s code.

D. These tables contain metadata that can be queried to gain additional helpful information.

Correct Answer: D

Reference: http://www.rackspace.com/knowledge_center/article/sql-injection-in-mysql