PT0-002^{Q&As}

PT0-002^{Q&As}

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.passapply.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A company\\'s Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi\\'s router. Which of the following is MOST vulnerable to a brute-force attack?

A. WPS

B. WPA2-EAP

C. WPA-TKIP

D. WPA2-PSK

Correct Answer: A

Reference: https://us-cert.cisa.gov/ncas/alerts/TA12-006A

QUESTION 2

During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

A. Deny that the vulnerability existed

B. Investigate the penetration tester.

C. Accept that the client was right.

D. Fire the penetration tester.

Correct Answer: B

QUESTION 3

Given the following script:

```
Line
1       #!/usr/bin/python3

Line
2       from scapy.all import *

Line a =
3       IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))

Line
4       b = sr1(a, verbose=0)

Line
5       for x in range(b[DNS].count):

Line
6         print(b[DNSRR][x].rdata
```

Which of the following BEST characterizes the function performed by lines 5 and 6?

A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10

B. Performs a single DNS query for www.comptia.org and prints the raw data output

C. Loops through variable b to count the results returned for the DNS query and prints that count to screen

D. Prints each DNS query result already stored in variable b

Correct Answer: D

QUESTION 4

A penetration tester joins the assessment team in the middle of the assessment. The client has asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

A. Prohibiting exploitation in the production environment

B. Requiring all testers to review the scoping document carefully

C. Never assessing the production networks

D. Prohibiting testers from joining the team during the assessment

Correct Answer: B

QUESTION 5

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign.

Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client\\'s cybersecurity tools? (Choose two.)

A. Scraping social media sites

B. Using the WHOIS lookup tool

C. Crawling the client\\'s website

D. Phishing company employees

E. Utilizing DNS lookup tools

F. Conducting wardriving near the client facility

Correct Answer: AC

Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.