PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.passapply.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?

A. nc looalhot 4423

B. nc -nvlp 4423 -?/bin/bash

C. nc 10.0.0.1 4423

D. nc 127.0.0.1 4423 -e /bin/bash

Correct Answer: B

QUESTION 2

A penetration tester, who is not on the client\\'s network. is using Nmap to scan the network for hosts that are in scope. The penetration tester is not receiving any response on the command:

nmap 100.100/1/0-125

Which of the following commands would be BEST to return results?

A. nmap -Pn -sT 100.100.1.0-125

B. nmap -sF -p 100.100.1.0-125

C. nmap -sV -oA output 100.100.10-125

D. nmap 100.100.1.0-125 -T4

Correct Answer: A

QUESTION 3

A company decides to remediate issues identified from a third-party penetration test done to its infrastructure. Management should instruct the IT team to:

A. execute the hot fixes immediately to all vulnerabilities found.

B. execute the hot fixes immediately to some vulnerabilities.

C. execute the hot fixes during the routine quarterly patching.

D. evaluate the vulnerabilities found and execute the hot fixes.

Correct Answer: D

QUESTION 4

A penetration test was performed by an on-staff junior technician. During the test, the technician discovered the web application could disclose an SQL table with user account and password information.

Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.

B. Connect to the SQL server using this information and change the password to one or two non-critical accounts to demonstrate a proof--of-concept to management.

C. Notify the development team of the discovery and suggest that input validation be implemented with a professional penetration testing company.

D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Correct Answer: A

QUESTION 5

After performing a security assessment for a firm, the client was found to have been billed for the time the client\\'s test environment was unavailable The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

A. SOW

B. NDA

C. EULA

D. BPA

Correct Answer: D