# 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**

When communicating the findings of a network vulnerability scan to a client\\'s IT department which of the following metrics BEST prioritize the severity of the findings? (Select TWO)

A. Threat map statistics

B. CVSS scores

C. Versions of affected software

D. Media coverage prevalence

E. Impact criticality

F. Ease of remediation

Correct Answer: BE

**QUESTION 2**

A penetration test was performed by an on-staff technicians junior technician. During the test, the technician discovered the 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 Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation 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 on the web application\\'s SQL query strings.

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

Correct Answer: A

**QUESTION 3**

Which of the following commands will allow a tester to enumerate potential unquoted service paths on a host?

A. wmic environment get name, variablevalue, username | findstr /i "Path" | findstr /i "Service"

B. wmic service get /format:hform > c:\temp\services.html

C. wmic startup get caption, location, command |findstr /i "service" |findstr /v /i "%"

D. wmic service get name, displayname, pathname, startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v """

Correct Answer: D

Reference: https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae

**QUESTION 4**

A penetration tester obtained access to an internal host of a given target. Which of the following is the BEST tool to retrieve the passwords of users of the machine exploiting a well-knows architecture flaw of the Windows OS?

A. Mimikatz

B. John the Ripper

C. RainCrack

D. Hashcat

Correct Answer: A

**QUESTION 5**

A penetration tester calls human resources and begins asking open-ended questions Which of the following social engineering techniques is the penetration tester using?

A. Interrogation

B. Elicitation

C. Impersonation

D. Spear phishing

Correct Answer: B