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.leads4pass.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

An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

A. Selection of the appropriate set of security testing tools

B. Current and load ratings of the ICS components

C. Potential operational and safety hazards

D. Electrical certification of hardware used in the test

Correct Answer: A

QUESTION 2

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

A. Advanced persistent threat

B. Script kiddie

C. Hacktivist

D. Organized crime

Correct Answer: B

Reference https://www.sciencedirect.com/topics/computer-science/disgruntled-employee

QUESTION 3

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A. dig -q any _kerberos._tcp.internal.comptia.net

B. dig -q any _lanman._tcp.internal.comptia.net

C. dig -q any _ntlm._tcp.internal.comptia.net

D. dig -q any _smtp._tcp.internal.comptia.net

Correct Answer: A

QUESTION 4

A penetration tester is connected to a client\\'s local network and wants to passively identify cleartext protocols and potentially sensitive data being communicated across the network. Which of the following is the BEST approach to take?

A. Run a network vulnerability scan.

B. Run a stress test.

C. Run an MITM attack.

D. Run a port scan.

Correct Answer: C

Reference: https://www.sciencedirect.com/topics/computer-science/encrypted-protocol

QUESTION 5

When conducting reconnaissance against a target, which of the following should be used to avoid directory communicating with the target?

A. Nmap tool

B. Maltego community edition

C. Nessus vulnerability scanner

D. OpenVAS

E. Melasploit

Correct Answer: B