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.geekcert.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 hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

QUESTION 2

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

A. Dictionary

B. Directory

C. Symlink

D. Catalog

E. For-loop

Correct Answer: A

A dictionary can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools. A dictionary is a collection of key- value pairs that can be accessed by using the keys. For example, a dictionary can store usernames and passwords, or IP addresses and hostnames, that can be used as input for brute-force or reconnaissance tools.

QUESTION 3

During an engagement, a penetration tester found the following list of strings inside a file: Which of the following is the BEST technique to determine the known plaintext of the strings?

3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17

A. Dictionary attack

B. Rainbow table attack

C. Brute-force attack

D. Credential-stuffing attack

Correct Answer: B

QUESTION 4

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

Pre-engagement interaction (scoping and ROE) Intelligence gathering (reconnaissance) Threat modeling Vulnerability analysis Exploitation and post exploitation Reporting

Which of the following methodologies does the client use?

A. OWASP Web Security Testing Guide

B. PTES technical guidelines

C. NIST SP 800-115

D. OSSTMM

Correct Answer: B

Reference: https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to- ptes/

QUESTION 5

A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client\\'s expectations?

A. OWASP Top 10

B. MITRE ATTandCK framework

C. NIST Cybersecurity Framework

D. The Diamond Model of Intrusion Analysis

Correct Answer: B

The MITRE ATTandCK framework is a methodology that should be used to best meet the client\\'s expectations. The MITRE ATTandCK framework is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are continuously updated based on real-world observations. The framework covers a wide variety of enterprise systems and networks, such as Windows, Linux, macOS, cloud, mobile, and network devices. The framework can help the penetration tester to emulate realistic threats and identify gaps in defenses.

PT0-002 VCE Dumps   PT0-002 Study Guide   PT0-002 Exam Questions