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.pass4itsure.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding

B. The network location of the vulnerable device

C. The vulnerability identifier

D. The client acceptance form

E. The name of the person who found the flaw

F. The tool used to find the issue

Correct Answer: CF

QUESTION 2

A penetration tester is conducting an on-path link layer attack in order to take control of a key fob that controls an electric vehicle. Which of the following wireless attacks would allow a penetration tester to achieve a successful attack?

A. Bluejacking

B. Bluesnarfing

C. BLE attack

D. WPS PIN attack

Correct Answer: C

A BLE (Bluetooth Low Energy) attack is specifically designed to exploit vulnerabilities in the Bluetooth Low Energy protocol, which is commonly used in modern wireless devices, including key fobs for electric vehicles. This type of attack can allow a penetration tester to intercept, manipulate, or take control of the communication between the key fob and the vehicle. Bluejacking and Bluesnarfing are older Bluetooth attacks that are less effective against modern BLE implementations. WPS PIN attacks target Wi- Fi Protected Setup, which is unrelated to key fobs and electric vehicles.

QUESTION 3

Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used

B. Bill of materials including supplies, subcontracts, and costs incurred during assessment

C. Quantitative impact assessments given a successful software compromise

D. Code context for instances of unsafe type-casting operations

Correct Answer: D

Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type- casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

QUESTION 4

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

A. Redirecting output from a file to a remote system

B. Building a scheduled task for execution

C. Mapping a share to a remote system

D. Executing a file on the remote system

E. Creating a new process on all domain systems

F. Setting up a reverse shell from a remote system

G. Adding an additional IP address on the compromised system

Correct Answer: CD

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

QUESTION 5

Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++

B. +val

C. val=(val+1)

D. ++val

E. val=val++

F. val+=1

Correct Answer: CF

In Python, there are two ways to increase a variable by one: using the assignment operator (=) with an arithmetic expression, or using the augmented assignment operator (+=). The expressions val=(val+1) and val+=1 both achieve this goal. The expressions val++ and ++val are not valid in Python, as there is no increment operator. The expressions +val and val=val++ do not change the value of val2. https://pythonguides.com/increment-and-decrement-operators-in-python/