GPEN$^{\text{Q\&As}}$

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gpen.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

The resulting business impact, of the penetration test or ethical hacking engagement is explained in what section of the final report?

A. Problems

B. Findings

C. Impact Assessment

D. Executive Summary

Correct Answer: D

Reference: http://www.frost.com/upld/get-data.do?id=1568233

QUESTION 2

Which of the following tools is a wireless sniffer and analyzer that works on the Windows operating system?

A. Void11

B. Airsnort

C. Kismet

D. Aeropeek

Correct Answer: D

QUESTION 3

Which Metasploit payload includes simple upload and download functionality for moving files to and from compromised systems?

A. DLL inject

B. Upexec

C. Meterpreter

D. Vncinject

Correct Answer: C

Meterpreter is the Metasploit payload that includes simple upload and download functionality for moving files to and from compromised systems. Meterpreter is an advanced, dynamically extensible payload that offers features such as file manipulation, network pivoting, and in-memory execution of shellcode. It is designed to operate within the memory of the compromised host, leaving a minimal footprint, and provides a high degree of control over the system. One of its key features is the ability to upload and download files, which is essential for effective control and information extraction during penetration testing or ethical hacking operations.

QUESTION 4

Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature. Which of the following statements is true in context with the above scenario?

A. Alternate Data Streams is a feature of Linux operating system.

B. Adam\\'s system runs on Microsoft Windows 98 operating system.

C. Adam is using FAT file system.

D. Adam is using NTFS file system.

Correct Answer: D

QUESTION 5

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration.

The tool uses raw IP packets to determine the following:

What ports are open on our network systems.

What hosts are available on the network.

Identify unauthorized wireless access points.

What services (application name and version) those hosts are offering.

What operating systems (and OS versions) they are running.

What type of packet filters/firewalls are in use.

Which of the following tools is Victor using?

A. Nmap

B. Kismet

C. Sniffer

D. Nessus

Correct Answer: A

GPEN Practice Test GPEN Exam Questions GPEN Braindumps