# GPEN 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.pass2lead.com/gpen.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

A. Use the getuid command to determine the user context the process is runningunder, then use the imp command to impersonate that user.

B. use the getpid command to determine the user context the process is runningunder, then use the Imp command to impersonate that user.

C. Use the execute command to the passmgr executable. That will give you access to the file.

D. Use the migrate command to jump to the passmgr process. That will give you accessto the file.

Correct Answer: C

**QUESTION 2**

Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow

B. Web ripping

C. DoS

D. Sniffing

Correct Answer: D

**QUESTION 3**

You are conducting a penetration test for a private company located in Canada. The scope extends to all internal-facing hosts controlled by the company. You have gathered necessary hold-harmless and non-disclosure agreements. Which action by your group can incur criminal liability under Criminal Code of Canada Sections 184 and 542 CC 184?

A. Analyzing internal firewall router software for vulnerabilities

B. Exploiting application vulnerabilities on end-user workstations

C. Attempting to crack passwords on a development server

D. Capturing a VoIP call to a third party without prior notice

Correct Answer: D

**QUESTION 4**

Which of the following statements are true about session hijacking?

Each correct answer represents a complete solution. Choose all that apply.

A. It is used to slow the working of victim\\'s network resources.

B. TCP session hijacking is when a hacker takes over a TCP session between two machines.

C. Use of a long random number or string as the session key reduces session hijacking.

D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Correct Answer: BCD

**QUESTION 5**

How many bits encryption does SHA-1 use?

A. 128

B. 140

C. 512

D. 160

Correct Answer: D