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.geekcert.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

QUESTION 1

You want to search the Apache Web server having version 2.0 using google hacking. Which of the following search queries will you use?

A. intitle:"Test Page for Apache Installation" "You are free"

B. intitle:"Test Page for Apache Installation" "It worked!"

C. intitle:test.page "Hey, it worked !" "SSl/TLS aware"

D. intitle:Sample.page.for.Apache Apache.Hook.Function

Correct Answer: D

QUESTION 2

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 3

Which of the following Web authentication techniques uses a single sign-on scheme?

A. Basic authentication

B. Digest authentication

C. NTLM authentication

D. Microsoft Passport authentication

Correct Answer: D

QUESTION 4

Which of the following is the second half of the LAN manager Hash?

A. 0xAAD3B435B51404BB

B. 0xAAD3B435B51404CC

C. 0xAAD3B435B51404EE

D. 0xAAD3B435B51404AA

Correct Answer: C

QUESTION 5

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

A. Post-attack phase

B. Attack phase

C. On-attack phase

D. Pre-attack phase

Correct Answer: D

GPEN VCE Dumps   GPEN Practice Test   GPEN Study Guide