# 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.pass4itsure.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 been contracted to perform a black box pen test against the Internet facing servers for a company. They want to know, with a high level of confidence, if their servers are vulnerable to external attacks. Your contract states that you can use all tools available to you to pen test the systems. What course of action would you use to generate a report with the lowest false positive rate?

A. Use a port scanner to find open service ports and generate a report listing allvulnerabilities associated with those listening services.

B. Use a vulnerability or port scanner to find listening services and then try to exploitthose services.

C. Use a vulnerability scanner to generate a report of vulnerable services.

D. Log into the system and record the patch levels of each service then generate areport that lists known vulnerabilities for all the running services.

Correct Answer: B

**QUESTION 2**

Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Stalking Amendment Act (1999)

B. Malicious Communications Act (1998)

C. Anti-Cyber-Stalking law (1999)

D. Stalking by Electronic Communications Act (2001)

Correct Answer: A

**QUESTION 3**

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server.

The output of the scanning test is as follows:

```
C:\whisker.pl -h target_IP_address

-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =

= Host: target_IP_address

= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1

mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22

+
```

200 OK: HEAD /cgi-bin/printenv John recognizes /cgi-bin/printenv vulnerability (\\'Printenv\\' vulnerability) in the We_are_secure server. Which of the following statements about \\'Printenv\\' vulnerability are true? Each correct answer represents a complete solution. Choose all that apply.

A.

\\'Printenv\\' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

B.

The countermeasure to \\'printenv\\' vulnerability is to remove the CGI script.

C.

This vulnerability helps in a cross site scripting attack.

D.

With the help of \\'printenv\\' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: BCD

**QUESTION 4**

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

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

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

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

Correct Answer: A

**QUESTION 5**

You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -B

B. tcpdump -dd

C. tcpdump -w

D. tcpdump –d

Correct Answer: C