GPEN^{Q&As}

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.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

QUESTION 1

While scanning a remote system that is running a web server with a UDP scan and monitoring the scan with a sniffer, you notice that the target is responding with ICMP Port Unreachable only once a second What operating system is the target likely running?

A. Linux

B. Windows

C. OpenBSD

D. Mac OS X

Correct Answer: A

QUESTION 2

Analyze the command output below. What action is being performed by the tester?

```
C:\>net use \\10.0.1.4\ipc$ "" /user:""
The command completed successfully.

C:\>user2sid \\10.0.1.4 Administrator

S-1-5-21-2571679061-1291049315-3862896415-500

Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\>user2sid \\10.0.1.4 sfarr

S-1-5-21-2571679061-1291049315-3862896415-1124

Number of subauthorities is 5
Domain is TEST-DOMAIN.COM
Length of SID in memory is 28 byte:
Type of SID is SidTypeUser
```

A. Creating user accounts on 10.0.1.4 and testing privileges

B. Collecting password hashes for users on 10.0.1.4

C. Attempting to exploit windows File and Print Sharing service

D. Gathering Security identifiers for accounts on 10.0.1.4

Correct Answer: D

QUESTION 3

Which of the following is the JavaScript variable used to store a cookie?

A. Browsercookie

B. Windowcookie

C. Document cookie

D. Session cookie

Correct Answer: C

Reference: http://www.w3schools.com/js/js_cookies.asp

QUESTION 4

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value. What may be the reason?

A. The zombie computer is not connected to the we-are-secure.com Web server.

B. The zombie computer is the system interacting with some other system besides your comp uter.

C. Hping does not perform idle scanning.

D. The firewall is blocking the scanning process.

Correct Answer: B

QUESTION 5

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