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

QUESTION 1

Which of the following is a web ripping tool?

A. Netcat

B. NetBus

C. SuperScan

D. Black Widow

Correct Answer: D

QUESTION 2

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-aresecure server. Which of the following are countermeasures against a brute force attack? Each correct answer represents a complete solution. Choose all that apply.

A. The site should increase the encryption key length of the password.

B. The site should restrict the number of login attempts to only three times.

C. The site should force its users to change their passwords from time to time.

D. The site should use CAPTCHA after a specific number of failed login attempts.

Correct Answer: BD

QUESTION 3

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com\\' and press the submit button. The

Web application displays the server error.

What can be the reason of the error?

A. The remote server is down.

B. You have entered any special character in email.

C. Your internet connection is slow.

D. Email entered is not valid.

Correct Answer: B

QUESTION 4

You have obtained the hash below from the /etc/shadow file. What are you able to discern simply by looking at this hash?

```
$1$uWeOhL6k$A4XDsB4COGqWaEpFjLLDe.
```

A. A4XD$B4COCqWaEpFjLLDe. is a SHAI hash that was created using the salt $1 SuWeOhL6k$ 1

B. A4XD$B4COCqWaEpFjLLDe. is an MD5 hash that was created using the salt $1 SuWeOhL6k$

C. A4XDsB4COGqWaEpFjLLDe. is an MD5 hash that was created using the salt uWeOhL6k

D. A4XDsB4COCqWaEpFjLLDe. is a SHAI hash that was created using the salt uweohL6k

Correct Answer: C

QUESTION 5

Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack

B. Cross-Site Scripting attack

C. Cross-Site Request Forgery

D. Code injection attack

Correct Answer: D

QUESTION 6

Which of the following federal laws are related to hacking activities? Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030

B. 18 U.S.C. 1028

C. 18 U.S.C. 2510

D. 18 U.S.C. 1029

Correct Answer: ACD

QUESTION 7

Which of the following best explains why you would warn to clear browser slate (history. cache, and cookies) between examinations of web servers when you\\'ve been trapping and altering values with a non-transparent proxy?

A. Values trapped and stored in the browser will reveal the techniques you\\'ve used toexamine the web servers.

B. Trapping and changing response values is beneficial for web site testing but usingthe same cached values in your browser will prevent you from being able to changethose values.

C. Trapping and changing response values is beneficial for web site testing but willcause browser instability if not cleared.

D. Values trapped and changed in the proxy, such as a cookie, will be stored by thebrowser and may impact further testing.

Correct Answer: D

QUESTION 8

You work as an IT Technician for uCertify Inc. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company\\'s wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. MAC Filtering

B. SSID

C. RAS

D. WEP

Correct Answer: A

QUESTION 9

When DNS is being used for load balancing, why would a penetration tester choose to identify a scan target by its IP address rather than its host name?

A. Asingle IP may have multiple domains.

B. A single domain name can only have one IP address.

C. Scanning tools only recognize IP addresses

D. A single domain name may have multiple IP addresses.

Correct Answer: C

Reference: http://www.flashcardmachine.com/sec-midterm.html

QUESTION 10

You work as an Administrator for Bluesky Inc. The company has 145 Windows XP Professional client computers and eighty Windows 2003 Server computers. You want to install a security layer of WAP specifically designed for a wireless environment. You also want to ensure that the security layer provides privacy, data integrity, and authentication for client-server communications over a wireless network. Moreover, you want a client and server to be authenticated so that wireless transactions remain secure and the connection is encrypted. Which of the following options will you use to accomplish the task?

A. Wired Equivalent Privacy (WEP)

B. Virtual Private Network (VPN)

C. Wireless Transport Layer Security (WTLS)

D. Recovery Console

Correct Answer: C

QUESTION 11

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement WPA

C. Don\\'t broadcast SSID

D. Implement MAC filtering

Correct Answer: C

QUESTION 12

Which of the following vulnerability scanner scans from CGI, IDA, Unicode, and Nimda vulnerabilities?

A. Hackbot

B. SARA

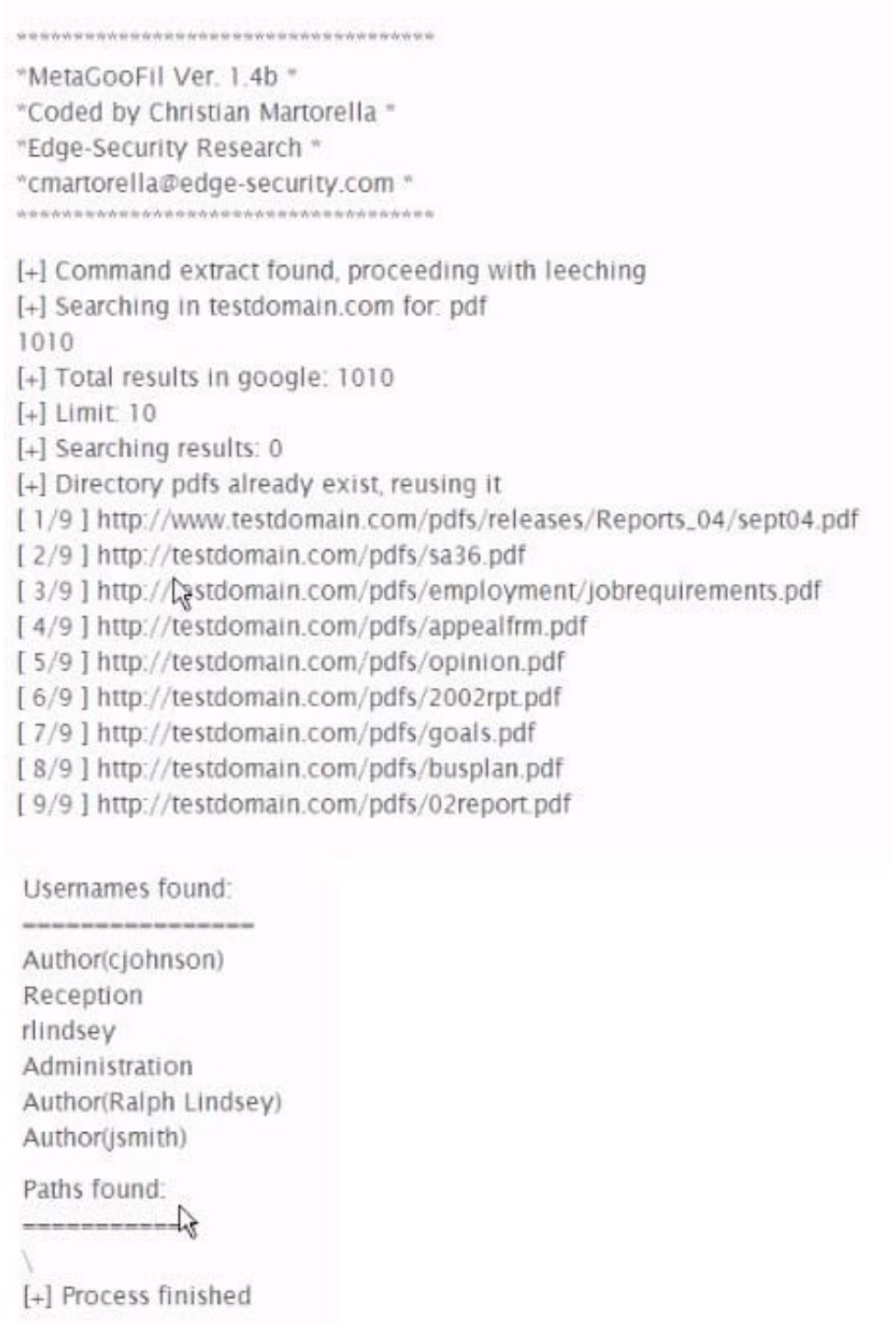
C. Nessus

D. Cgichk

Correct Answer: A

QUESTION 13

Analyze the command output below. What information can the tester infer directly from the Information shown?



A. Usernames for the domain tesrdomain.com

B. Directory indexing is allowed on the web server

C. Vulnerable versions of Adobe software in use

D. Naming convention for public documents

Correct Answer: D

QUESTION 14

Fill in the blank with the appropriate tool.

____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

A. NBTscan

Correct Answer: A

QUESTION 15

You want to connect to your friend\\'s computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

A. Remoxec

B. Hk.exe

C. PSExec

D. GetAdmin.exe

Correct Answer: C