GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gcih.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 primary outcome of an effective Incident Handling program?

A. Reduced time between system outage and service restoration or alternate resources brought online.

B. Critical systems are identified and assigned a business owner.

C. Reduced time between detecting an adverse system event and when the root cause is addressed.

D. Critical systems are backed up and restores are tested regularly.

Correct Answer: A

QUESTION 2

Which of the following malicious software travels across computer networks without the assistance of a user?

A. Worm

B. Virus

C. Hoax

D. Trojan horses

Correct Answer: A

QUESTION 3

What is the goal of the command sequence shown below? >nslookup

>server [authoritative_server_IP_or_name]

>set type=any

>ls -d [target_domain]

A. Arp Spoofing

B. Zone Transfer

C. DNS Cache Poisoning

D. IP Spoofing

Correct Answer: B

QUESTION 4

Which of the following commands will enumerate a list of shares on a Windows target machine?

A. net share \\192.168.99.133

B. net view \\192.168.99.133

C. net use \\192.168.99.133

D. net session \\192.168.99.133

Correct Answer: B

QUESTION 5

Your CIO, Thomas Fischer, has complained that vendors are cold calling him to get more information about your organization\\'s new domain name (tvf-prod.com). You\\'ve extracted the information below from tvf-prod.com. What should you report back to the CIO?

```
   Domain Name: TVF-PROD.COM
   Registrar: GODADDY.COM, INC.
   Whois Server: whois.godaddy.com
   Referral URL: http://registrar.godaddy.com
   Name Server: NS23.DOMAINCONTROL.COM
   Name Server: NS24.DOMAINCONTROL.COM
   Status: clientDeleteProhibited
   Status: clientRenewProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 23-nov-2010
   Creation Date: 12-feb-2002
   Expiration Date: 12-feb-2013

>>> Last update of whois database: Fri, 12 Aug 2011 13:30:15 UTC <<<

Registrant:
   TVF Productions
   22 rue anonyme
   Ville 90000
   France

   Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
   Domain Name: TVF-PROD.COM
      Created on: 12-Feb-02
      Expires on: 12-Feb-13
      Last Updated on: 23-Nov-10

   Administrative Contact:
      Fischer, Thomas  tvfi@baddomain.com
      TVF Productions
      22 rue anonyme
      Ville 90000
      France
      5551234567       Fax --

   Technical Contact:
      Fischer, Thomas  tvfi@baddomain.com
      TVF Productions
      22 rue anonyme
      Ville 90000
      France
      5551234567       Fax --

   Domain servers in listed order:
```

A. His contact information was linked to the new domain in WHOIS, and should be changed to your organization\\'s generic registration data

B. His contact information has been published in the WHOIS database, and since Internic manages this information, it cannot be removed

C. His contact information has been published on the new website, and the marketing department should remove it

D. Someone outside the organization has published his contact information, and he should run a Google search to track down the offender

Correct Answer: A

The extract represents the information for the new domain name from WHOIS. The extract clearly shows that his personal data has been published in association with the new domain, which represents the most likely sources of the phone calls. These should be changed to remove the number and put a generic email address. Although the data may have been published by parties external to the company or on a new website, these are not necessarily linked to the new Internet domain. The management of the WHOIS data is usually the responsibility of the company registering the domain name and they can change it themselves.