



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.geekcert.com/gcih.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

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks? Each correct answer represents a complete solution. (Choose all that apply.)

- A. Hybrid attack
- B. Rule based attack
- C. Dictionary attack
- D. Brute Force attack

Correct Answer: ACD

QUESTION 2

Which of the following protocols uses only User Datagram Protocol (UDP)?

- A. POP3
- B. FTP
- C. ICMP
- D. TFTP

Correct Answer: D

QUESTION 3

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The company has three Windows 2008 file servers, 150 Windows XP Professional,

thirty UNIX-based client computers. The network users have identical user accounts for both Active Directory and the UNIX realm. You want to ensure that the UNIX clients on the network can access the file servers. You also want to ensure

that the users are able to access all resources by logging on only once, and that no additional software is installed on the UNIX clients.

What will you do to accomplish this task?

Each correct answer represents a part of the solution. (Choose two.)

- A. Configure a distributed file system (Dfs) on the file server in the network.
- B. Enable the Network File System (NFS) component on the file servers in the network.
- C. Configure ADRMS on the file servers in the network.



D. Enable User Name Mapping on the file servers in the network.

Correct Answer: BD

QUESTION 4

Canaries help to implement what protective mechanisms in the stack?

- A. Availability
- B. Confidentiality
- C. Secrecy
- D. Integrity

Correct Answer: D

When the return pointer gets pushed on the stack, the system calculates a keyed hash of the return pointer. This keyed hash result, known as a canary, will be used later as an integrity check of the return pointer to make sure it hasn't been altered by an attacker.

QUESTION 5

Analyze the data shown below. Where does this data originate from?

```
? (172.16.62.254) at 00:50:56:e8:b1:4b [ether] on eth0  
? (172.16.62.2) at 00:50:56:e8:68:e7 [ether] on eth0  
? (172.16.62.84) at 04:b0:77:81:90:5f [ether] on eth0  
? (172.16.62.102) at 30:40:50:d3:14:af [ether] on eth0
```

- A. Established connections
- B. Routing table
- C. ARP cache
- D. Network interfaces

Correct Answer: C

Reference: https://petri.com/csc_arp_cache

[GCIH PDF Dumps](#)

[GCIH Exam Questions](#)

[GCIH Braindumps](#)