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.pass4itsure.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 techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

A. MAC spoofing

B. IP address spoofing

C. Email spoofing

D. ARP spoofing

Correct Answer: D

QUESTION 2

Victor works as a professional Ethical Hacker for ABC Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information? Each correct answer represents a complete solution. (Choose all that apply.)

A. Slack space

B. Hidden partition

C. Dumb space

D. Unused Sectors

Correct Answer: ABD

QUESTION 3

Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

A. rkhunter

B. OSSEC

C. chkrootkit

D. Blue Pill

Correct Answer: C

QUESTION 4

Which of the following user accounts is the default Administrator account?

```
rpcclient $> enumdomusers
user:[DefaultAccount] rid:[0x1f7]
user:[Guest] rid:[0x1f5]
user:[JustAnotherUser] rid:[0x1fA]
user:[JoePowershell] rid:[0x1f4]
user:[JaneSamba] rid:[0x1f8]
user:[JeremyIIS] rid:[0x1ga]
```

A. JustAnotherUser

B. JoePowershell

C. JaneSamba

D. JeremyIIS

Correct Answer: B

QUESTION 5

After a system that was compromised in an incident is brought back into production, which part of the incident handling process must be done?

A. Wipe and reinstall from original media

B. Monitor for compromise

C. Create a baseline

D. Create a new, clean, backup

E. Reinstall from last uncompromised backup

Correct Answer: B

If the eradication was not complete or the infection vector was not closed off, the earlier you detect re-infection, the better off everyone is. It is also politically better if the handlers detect the problem and show up to fix it than if the problem comes to light because business operations are affected. This is a serious problem. Many times, handlers take some shortcut along the way, or there is something you never discovered about the attack vector, and the problem comes back.