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.pass2lead.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

Which of the following is the most effective at eradicating a system infected with a Rootkit?

A. Disable the rootkit service in Control Panel/Administrative Tools/Services

B. Format the drive, reinstall the OS applying any applicable patches, and change passwords

C. Uninstall the Rootkit via Add / Remove Programs

D. Delete the rootkit files and remove the startup shortcut

Correct Answer: C

QUESTION 2

Which of the following is the most common vulnerability that can affect desktop applications written in native code?

A. SpyWare

B. DDoS attack

C. Malware

D. Buffer overflow

Correct Answer: D

QUESTION 3

What is one of the functions CyberCPR performs?

A. It can act as a NIDS when traffic is routed through it

B. All uploaded files are hashed

C. CyperCPR can act as an secure email server

D. It can act as a HIDS on the system it is installed on

Correct Answer: A

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

What is the goal of the containment phase of incident handling?

A. Monitoring the attacker to gather data on the progress of the attack

B. Analyzing a system to determine if an incident has occurred

C. Preventing the attacker from further compromising systems

D. Removing all artifacts of the attacker from the impacted system

Correct Answer: C