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.leads4pass.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 systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

A. US Incident Management System (USIMS)

B. National Disaster Management System (NDMS)

C. National Emergency Management System (NEMS)

D. National Incident Management System (NIMS)

Correct Answer: D

QUESTION 2

What information is commonly found in both the header and the possession log of a Chain of Custody?

A. Date and time the evidence was requested by the court

B. Date and time the evidence was checked into evidence locker

C. Date and time the evidence was initially collected

D. Date and time the evidence is classified as reliable

Correct Answer: B

QUESTION 3

Which of the following hacking tools provides shell access over ICMP?

A. John the Ripper

B. Nmap

C. Nessus

D. Loki

Correct Answer: D

QUESTION 4

What task is the Linux administrator performing with the command below? python dpat.py -n ../ntdsbak/customer.ntds -c ../ntdsbak/hashcat.potfile -g ../ntdsbak/*.txt

A. Remove salts

B. Analyze password selections

C. Extract NT hashes

D. Crack passwords

Correct Answer: B

Reference: https://github.com/clr2of8/DPAT

QUESTION 5

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. (Choose two.)

A. Land attack

B. SYN flood attack

C. Teardrop attack

D. Ping of Death attack

Correct Answer: CD