GCIH$^{Q\&As}$

GIAC Certified Incident Handler

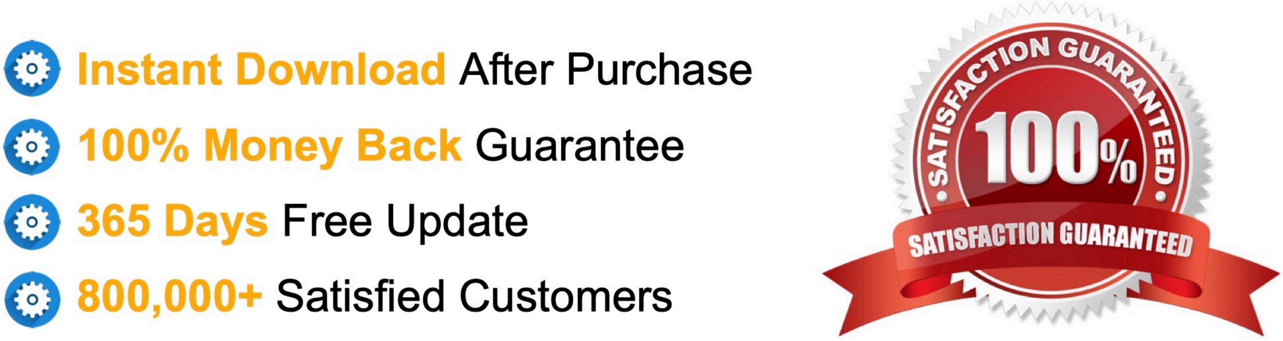
Pass GIAC GCIH Exam with 100% Guarantee

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



QUESTION 1

A host has been compromised with a rootkit through Internet activity. The analyst wishes to reconstruct the binary file used to infect the host. Which of the following sources of evidence is MOST likely to produce the binary?

A. Filesystem journal entries from the compromised host

B. Alert logs from an Intrusion detection device

C. A memory image from a proxy server on the network

D. Packet captures from a sensor at the network border

Correct Answer: D

Since the host was infected over the network, packet captures are the most likely location to find the original binary. Alert logs and filesystem journals will retain metadata and not the actual content.

QUESTION 2

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 3

Which of the following tools can be used to detect the steganography?

A. Dskprobe

B. Blindside

C. ImageHide

D. Snow

Correct Answer: A

QUESTION 4

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Whisker

B. Fragroute

C. Nessus

D. Y.A.T.

Correct Answer: AC

QUESTION 5

Which of the following methods can be used to detect session hijacking attack?

A. nmap

B. Brutus

C. ntop

D. sniffer

Correct Answer: D