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

QUESTION 1

Why do protocol parsers such as sniffers often run with root or system privileges?

A. So they can attach to port numbers higher than 1024 on Unix systems

B. So they can scan open files for application data

C. So they can run with application-level functionality

D. So they can run the network card in promiscuous mode

Correct Answer: D

Flaws in these protocol parsers let the attacker get the privileges of the vulnerable program. Often, these programs run with root or system privileges so they can grab packets in promiscuous mode, and/or so they can attach to a port number less than 1024 on Unix, and/or because they involve system-level functionality.

QUESTION 2

Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?

A. Ethercap

B. Tripwire

C. IPChains

D. Hunt

Correct Answer: D

QUESTION 3

Which of the following functions can you use to mitigate a command injection attack? Each correct answer represents a part of the solution. (Choose all that apply.)

A. escapeshellarg()

B. escapeshellcmd()

C. htmlentities()

D. strip_tags()

Correct Answer: AB

QUESTION 4

Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. SPI

B. Distributive firewall

C. Honey Pot

D. Internet bot

Correct Answer: A

QUESTION 5

Why should organizations consider disabling auto-run as part of their Windows system hardening baselines?

A. Disabling auto-run prevents data transfer from external media to the hard drive

B. To help prevent malware from spreading through external media

C. To eliminate the risk of connecting unauthorized wireless devices

D. To prevent users from copying sensitive data to external media

Correct Answer: B

On Windows systems, malware often copies an autorun.exe file to external media, so shared thumb drives are a common vector of infection for worms. Since the drive is still enables (but autorun is not), this would not prevent any user action from taking place. Auto-run does not change permissions on drives.