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

Which of the following protocols is a maintenance protocol and is normally considered a part of the IP layer, but has also been used to conduct denial-of-service attacks?

A. ICMP

B. L2TP

C. TCP

D. NNTP

Correct Answer: A

QUESTION 2

Which of the following is a reason to implement security logging on a DNS server?

A. For preventing malware attacks on a DNS server

B. For measuring a DNS server\\'s performance

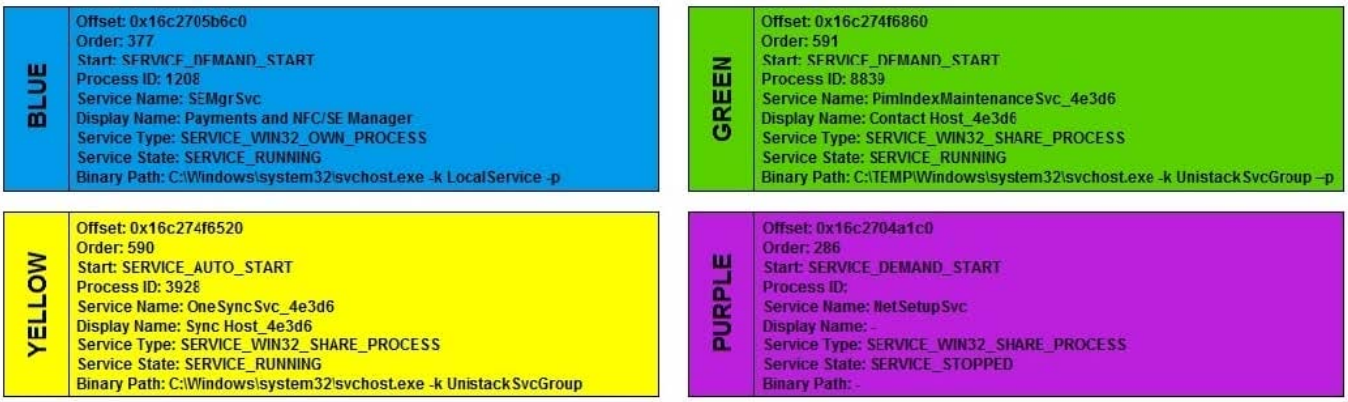
C. For monitoring unauthorized zone transfer

D. For recording the number of queries resolved

Correct Answer: C

QUESTION 3

Which of the following describes a suspicious event in the service data below? root@kali:~/volatility# ./vol.py -f ../mem/Desk005.vmem svcscan



A. GREEN: Executables should not be run from temporary folders

B. BLUE: Service names should be all capital letters

C. PURPLE: Services should not be in the STOPPED state

D. YELLOW: Option -k should be followed by -p for svchost

Correct Answer: D

QUESTION 4

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc. Recently, John\\'s company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:

alert(\\'Hi, John\\')

After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John." Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

A. Replay attack

B. CSRF attack

C. Buffer overflow attack

D. XSS attack

Correct Answer: D

QUESTION 5

Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason.

Which of the following mistakes made by Jason helped the Forensic Investigators catch him?

A. Jason did not perform a vulnerability assessment.

B. Jason did not perform OS fingerprinting.

C. Jason did not perform foot printing.

D. Jason did not perform covering tracks.

E. Jason did not perform port scanning.

Correct Answer: D