GCCC$^{\text{Q\&As}}$

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

IDS alerts at Service Industries are received by email. A typical day process over 300 emails with fewer than 50 requiring action. A recent attack was successful and went unnoticed due to the number of generated alerts.

What should be done to prevent this from recurring?

A. Tune the IDS rules to decrease false positives.

B. Increase the number of staff responsible for processing IDS alerts.

C. Change the alert method from email to text message.

D. Configure the IDS alerts to only alert on high priority systems.

Correct Answer: A

QUESTION 2

Which of the following should be used to test antivirus software?

A. FIPS 140-2

B. Code Red

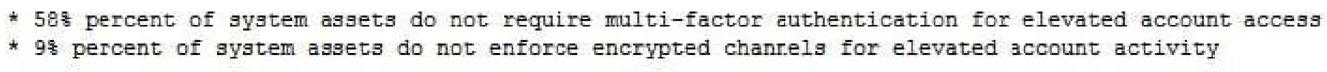
C. Heartbleed

D. EICAR

Correct Answer: D

QUESTION 3

Given the audit finding below, which CIS Control was being measured?



```
* 58% percent of system assets do not require multi-factor authentication for elevated account access
* 9% percent of system assets do not enforce encrypted channels for elevated account activity
```

A. Controlled Access Based on the Need to Know

B. Controlled Use of Administrative Privilege

C. Limitation and Control of Network Ports, Protocols and Services

D. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

E. Inventory and Control of Hardware Assets

Correct Answer: B

QUESTION 4

As part of an effort to implement a control on E-mail and Web Protections, an organization is monitoring their webserver traffic. Which event should they receive an alert on?

A. The number of website hits is higher that the daily average

B. The logfiles of the webserver are rotated and archived

C. The website does not respond to a SYN packet for 30 minutes

D. The website issues a RST to a client after the connection is idle

Correct Answer: C

QUESTION 5

Which of the following statements is appropriate in an incident response report?

A. There had been a storm on September 27th that may have caused a power surge

B. The registry entry was modified on September 29th at 22:37

C. The attacker may have been able to access the systems due to missing KB2965111

D. The backup process may have failed at 2345 due to lack of available bandwidth

Correct Answer: B