GCCC^{Q&As}

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gccc.html

100% Passing Guarantee
100% Money Back Assurance

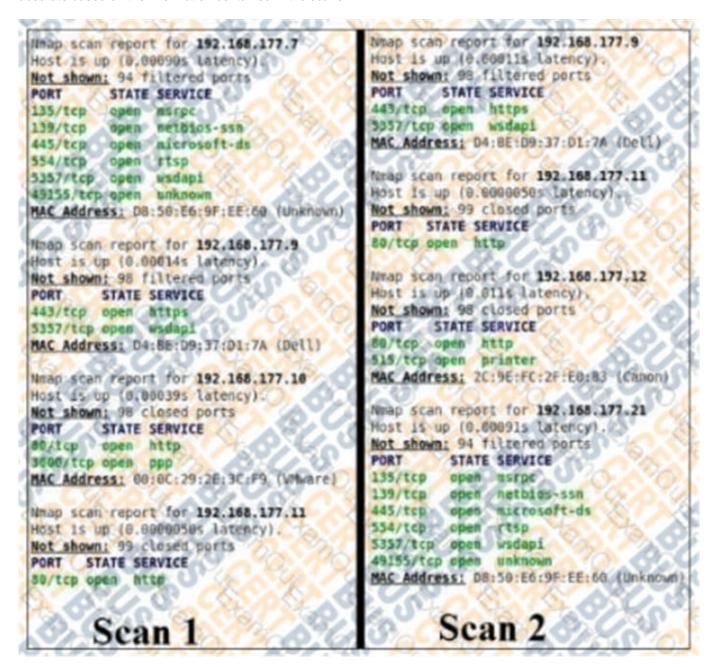Following Questions and Answers are all new published by GIAC
Official Exam Center

QUESTION 1

Scan 1 was taken on Monday. Scan 2 was taken of the same network on Wednesday. Which of the following findings is accurate based on the information contained in the scans?

A. The host located at 192.168.177.7 is no longer on the network

B. The host with MAC Address D8:50:E6:9F:EE:60 is no longer on the network

C. The host located at 192.168.177.21 is a new host on the network

D. The host with MAC Address D8:50:E6:9F:EE:60 had an IP address change

Correct Answer: D

QUESTION 2

Executive management approved the storage of sensitive data on smartphones and tablets as long as they were encrypted. Later a vulnerability was announced at an information security conference that allowed attackers to bypass the device\'s authentication process, making the data accessible. The smartphone manufacturer said it would take six months for the vulnerability to be fixed and distributed through the cellular carriers. Four months after the vulnerability was announced, an employee lost his tablet and the sensitive information became public.

What was the failure that led to the information being lost?

A. There was no risk acceptance review after the risk changed

B. The employees failed to maintain their devices at the most current software version

C. Vulnerability scans were not done to identify the devices that we at risk

D. Management had not insured against the possibility of the information being lost

Correct Answer: A

QUESTION 3

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 4

What tool creates visual network topology output and results that can be analyzed by Ndiff to determine if a service or network asset has changed?

A. Ngrep

B. CIS-CAT

C. Netscreen

D. Zenmap

Correct Answer: D

QUESTION 5

What could a security team use the command line tool Nmap for when implementing the Inventory and Control of Hardware Assets Control?

A. Control which devices can connect to the network

B. Passively identify new devices

C. Inventory offline databases

D. Actively identify new servers

Correct Answer: D