SY0-601 $^{\text{Q\&As}}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.passapply.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following can a security director use to prioritize vulnerability patching within a company\\'s IT environment?

A. SOAR

B. CVSS

C. SIEM

D. CVE

Correct Answer: B

QUESTION 2

A nationwide company is experiencing unauthorized logins at all hours of the day. The logins appear to originate from countries in which the company has no employees. Which of the following controls should the company consider using as part of its IAM strategy? (Select TWO).

A. A complex password policy

B. Geolocation

C. An impossible travel policy

D. Self-service password reset

E. Geofencing

F. Time-based logins

Correct Answer: AB

QUESTION 3

During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

A. The forensic investigator forgot to run a checksum on the disk image after creation

B. The chain of custody form did not note time zone offsets between transportation regions

C. The computer was turned off. and a RAM image could not be taken at the same time

D. The hard drive was not properly kept in an antistatic bag when rt was moved

Correct Answer: B

The question states that a trial Judge determined evidence gathered from a hard drive was not admissible. It is obvious that this is a legal matter. All of the remaining answers are of a technical nature, So consequently the only issue that a Judge can rule on is a Chain of custody issue. So, ladies and gentlemen, I rest my case (quickly bangs a gavel upon the desk)

QUESTION 4

A user contacts the help desk to report the following:

1.

Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID.

2.

This had never happened before, but the user entered the information as requested.

3.

The user was able to access the Internet but had trouble accessing the department share until the next day.

4.

The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point

B. Evil twin

C. DNS poisoning

D. ARP poisoning

Correct Answer: B

The person started seeing fraudulent bank activity after connecting to the wireless network. On top of that a rogue access point would most likely NOT have the same SSID as the corporate network.

https://security.stackexchange.com/questions/152816/whats-the-difference-between-an-evil-twin-and-a-rogue-access-point#:~:text=A%20rogue%20access%20point%20is,network%20or%20even%20to%20internet.

QUESTION 5

A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

A. PEAP

B. PSK

C. WPA3

D. WPS

Correct Answer: A

PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that can provide secure authentication for wireless networks. PEAP can use certificates to authenticate the server and the client, or only the server. PEAP can also use other methods, such as passwords or tokens, to authenticate the client. PEAP can ensure only employees with a valid certificate can authenticate to the network.