220-1102 Q&As

CompTIA A+ Certification Exam: Core 2

Pass CompTIA 220-1102 Exam with 100% Guarantee

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

https://www.geekcert.com/220-1102.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

A. A bad antivirus signature update was installed.

B. A router was misconfigured and was blocking traffic.

C. An upstream internet service provider was flapping.

D. The time or date was not in sync with the website.

Correct Answer: B

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

QUESTION 2

A technician is troubleshooting a Windows 10 PC that has experienced a BSOD. The user recently installed optional Windows updates. Which of the following is best way to resolve the issue?

A. Enable System Restore.

B. Roll back the device drivers.

C. Reinstall the OS.

D. Update the BIOS.

Correct Answer: B

To resolve a BSOD issue on a Windows 10 PC after installing optional Windows updates, the best approach is to Roll back the device drivers (B). BSODs can often be caused by incompatible or faulty drivers introduced during an update. Rolling back the drivers to a previous version can restore system stability and resolve the BSOD issue.

QUESTION 3

A user\\'s corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

A. Remote wipe

B. Firewall

C. Device encryption

D. Remote backup

E. Antivirus

F. Global Positioning System

Correct Answer: AC

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner. It is used to protect data from being compromised if the device is lost, stolen, or changed hands1. Device encryption is a

feature that helps protect the data on a device by making it unreadable to unauthorized users2. It requires a key or a password to access the data. Both features can help mitigate the risk of losing company trade secrets if a corporate phone

is stolen.

References:

How to remote wipe Windows laptop

(https://www.thewindowsclub.com/remote-wipe-windows-10)

Device encryption in Windows (https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d)

QUESTION 4

Which of the following is also known as something you know, something you have, and something you are?

A. ACL

B. MFA

C. SMS

D. NFC

Correct Answer: B

MFA stands for Multi-Factor Authentication, which is a method of verifying a user\\'s identity using two or more different factors of authentication. The three factors of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example: Something you know: a password, a PIN, a security question, etc. Something you have: a smart card, a token, a mobile device, etc. Something you are: a fingerprint, a face, an iris, etc. MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

QUESTION 5

A small library has an integrated switch and router that is not wireless. All of the public PCs in the library are connected to the device. Which of the following is the FIRST thing the library should do to deter curious patrons from interfering

with the device?

A. Configure DNS to resolve externally rather than internally

B. Enable MAC filtering to permit public PCs

C. Change the default user name and password

D. Set up the DHCP server to use a different gateway option

Correct Answer: C