- **Vendor: CompTIA**
- **Exam Code: SY0-501**
- **Exam Name: CompTIA Security+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in Oct./2020)**

QUESTION 1204
A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

A. Visitor logs
B. Cable locks
C. Guards
D. Disk encryption
E. Motion detection

Answer: B

QUESTION 1205
Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?

A. It increases the number of controls required to subvert a system
B. It decreases the time a CERT has to respond to a security incident.
C. It alleviates problems associated with EOL equipment replacement.
D. It allows for bandwidth upgrades to be made without user disruption.

Answer: A

QUESTION 1206
Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment.
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

Answer: A

QUESTION 1207
A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?

A. Network access control
B. Configuration manager
C. Application whitelisting
D. File integrity checks

Answer: C

QUESTION 1208
A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

Answer: E

QUESTION 1209
Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.
B. The test is performed against the wrong host.
C. The signature matches the product but not the version information.
D. The hosts are evaluated based on an OS-specific profile.

Answer: A

QUESTION 1210
An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address or mobile number to receive a code to access the data. Which of the following authentication methods did the organization implement?

A. Token key
B. Static code
C. Push notification
D. HOTP

Answer: D

QUESTION 1211
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

Answer: C

QUESTION 1212
Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicated an error.
B. The vendor has not published security patches recently.
C. The object has been removed from the Active Directory.
D. Logs show a performance degradation of the component.

Answer: B

QUESTION 1213
Using an ROT13 cipher to protect confidential information for unauthorized access is known as:

A. steganography.
B. obfuscation.
C. non-repudiation.
D. diffusion.

Answer: B

QUESTION 1214
A company is implementing a tool to mask all PII when moving data from a production server to a testing server. Which of the following security techniques is the company applying?

A. Data wiping
B. Steganography
C. Data obfuscation
D. Data sanitization

Answer: C