➢ **Vendor:** CompTIA

➢ **Exam Code:** SY0-501

➢ **Exam Name:** CompTIA Security+ Certification Exam

➢ **New Updated Questions from Braindump2go (Updated in June/2020)**

Visit Braindump2go and Download Full Version SY0-501 Exam Dumps

QUESTION 919
In order to prevent the possibility of a thermal shutdown. which of the following physical controls should be implemented in a datacenter?

A. Hot and cold aisles
B. Air-gapped servers
C. Infrared detection
D. Halon suppression

Answer: A

QUESTION 920
Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking
B. IP spoofing
C. Evil twin
D. ARP poisoning

Answer: D

QUESTION 921
A security analyst is running a credential-based vulnerability scanner on a Windows host. The vulnerability scanner is using the protocol NetBIOS over TCP/IP to connect to various systems. However, the scan does not return any results. To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135
B. 137
C. 3389
D. 5060

Answer: B

QUESTION 922
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: C

QUESTION 923
A company has a backup site with equipment on site without any data. This is an example of:

A. a hot site.
B. a cold site.
C. a hot standby.
D. a warm site.

Answer: D

QUESTION 924
A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning, and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR
B. FAR
C. CER
D. SLA

Answer: A

QUESTION 925
A technician is auditing network security by connecting a laptop to open hardwired jacks within the facility to verify they cannot connect. Which of the following is being tested?

A. Layer 3 routing
B. Port security
C. Secure IMAP
D. S/MIME

Answer: B

QUESTION 926
A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM.
Which of the following is the administrator protecting against?

A. VM sprawl
B. VM escape
C. VM migration
D. VM sandboxing

Answer: B

QUESTION 927
Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating
B. Corrective

C. Detective
D. Deterrent

Answer: D

QUESTION 928
Which of the following is a major disadvantage of ECB?

A. The encryption method is very resource intensive.
B. It is a proprietary algorithm, which can be expensive to implement.
C. It cannot be used with a PKI.
D. Identical plaintext values will yield the same ciphertext values.

Answer: D

QUESTION 929
A company is deploying a file-sharing protocol across a network and needs to select a protocol for authenticating clients, Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. Use MSCHAP authentication

Answer: C

QUESTION 930
An attacker has obtained the user ID and password of a data center's backup operator and has gained access to a production system.
Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.
B. Initiate a confidential data exfiltration process
C. Look for known vulnerabilities to escalate privileges
D. Create an alternate user ID to maintain persistent access

Answer: B