- **Vendor: CompTIA**
- **Exam Code: SY0-501**
- **Exam Name: CompTIA Security+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in May/2021)**

QUESTION 1388
A company wants to provide a guest wireless system for its visitors. The system should have a captive portal for guest self-registration and protect guest devices from spreading malware to other connected devices. Which of the following should be done on the wireless network to satisfy these requirements? (Choose two.)

A. Configure WPA2-PSK.
B. Configure a wireless IDS.
C. Use an open authentication system.
D. Enforce 802.1X with PEAP.
E. Disable SSID broadcasting.
F. Enable client isolation.

Answer: DF

QUESTION 1389
After a breach, a company has decided to implement a solution to better understand the technique used by the attackers. Which of the following is the BEST solution to be deployed?

A. Network analyzer
B. Protocol analyzer
C. Honeypot network
D. Configuration compliance scanner

Answer: C

QUESTION 1390
A security analyst is investigating a security breach involving the loss of sensitive data. A user passed the information through social media as vacation photos. Which of the following methods was used to encode the data?

A. Obfuscation
B. Steganography
C. Hashing
D. Elliptic curve

Answer: B

QUESTION 1391
When conducting a penetration test, a pivot is used to describe a scenario in which

A. the penetration tester uses pass-the-hash to gain access to a server via SMB, and then uses this server to SSH to another server.
B. a penetration tester is able to download the Active Directory database after exploiting an unpatched vulnerability on the domain controller
C. the vulnerability scanner reveals a flaw in SMB signing, which can be used to send a netcat recon tool to one of the servers on the network.
D. the penetration tester is able to access the datacenter or network closet by using a lockpick.

Answer: A

QUESTION 1392
A network administrator needs to restrict the users of the company's WAPs to the sales department. The network administrator changes and hides the SSID and then discovers several employees had connected their personal devices to the wireless network. Which of the following would limit access to the wireless network to only organization-owned devices in the sales department?

A. Implementing MAC filtering
B. Reducing the signal strength to encompass only the sales department
C. Replacing the APs and sales department wireless cards to support 802.11b
D. Issuing a BYOD policy

Answer: A

QUESTION 1393
A security engineer wants to further secure a sensitive VLAN on the network by introducing MFA. Which of the following is the BEST example of this?

A. PSK and PIN
B. RSA token and password
C. Fingerprint scanner and voice recognition
D. Secret question and CAPTCHA

Answer: B

QUESTION 1394
A malicious actor compromises a legitimate website, configuring it to deliver malware to visitors of the website. Which of the following attacks does this describe?

A. Whaling
B. Watering hole
C. Impersonation
D. Spoofing

Answer: B

QUESTION 1395
Which of the following BEST describes why an air gap is a useful security control?

A. It physically isolates two or more networks, therefore helping prevent cross contamination or accidental data spillage.
B. It requires that files be transferred via USB instead of networks that are potentially vulnerable to hacking, therefore preventing virus infections.
C. It requires multiple systems administrators with different credentials, therefore providing separation of duties.
D. It provides physical space between two interlocking doors, therefore providing additional control

from unauthorized entry.

Answer: A

QUESTION 1396
A security analyst is asked to check the configuration of the company's DNS service on the server. Which of the following command line tools should the analyst use to perform the initial assessment?

A. nslookup/dig
B. tracert
C. ipconfig/ifconfig
D. tcpdump

Answer: A

QUESTION 1397
A company help desk has received several reports that employees have experienced identity theft and compromised accounts. This occurred several days after receiving an email asking them to update their personal bank information. Which of the following is a vulnerability that has been exploited?

A. Trojan horses
B. Phishing
C. Improperly configured accounts
D. Forged certificates
E. Untrained users

Answer: E

QUESTION 1398
A systems administrator wants to enforce the use of HTTPS on a new website. Which of the following should the systems administrator do NEXT after generating the CSR?

A. Install the certificate on the server.
B. Provide the public key to the CA.
C. Password protect the public key.
D. Ensure the new key is not on the CRL.

Answer: A

QUESTION 1399
A penetration tester has been hired to scan a company's network for potentially active hosts. The company's IPS system blocks the ICMP echo reply and echo request packets. Which of the following can be used to scan the network?

A. OSPF
B. ARP
C. IPSec
D. Ping

Answer: B

QUESTION 1400
A company uses WPA2-PSK, and it appears there are multiple unauthorized devices connected to the wireless network. A technician suspects this is because the wireless password has been shared with unauthorized individuals. Which of the following should the technician implement to BEST reduce the risk of this happening in the future?

A. Wireless guest isolation
B. 802.1X
C. WPS
D. MAC address blacklist

Answer: B

QUESTION 1401
A new PKI is being built at a company, but the network administrator has concerns about spikes of traffic occurring twice a day due to clients checking the status of the certificates. Which of the following should be implemented to reduce the spikes in traffic?

A. CRL
B. OCSP
C. SAN
D. OID

Answer: B

QUESTION 1402
A security analyst received an after-hours alert indicating that a large number of accounts with the suffix "admin" were locked out. The accounts were all locked out after five unsuccessful login attempts, and no other accounts on the network triggered the same alert. Which of the following is the BEST explanation for these alerts?

A. The standard naming convention makes administrator accounts easy to identify and they were targeted for an attack.
B. The administrator accounts do not have rigid password complexity rules, and this made them easier to crack.
C. The company has implemented time-of-day restrictions, and this triggered a false positive alert when the administrators tried to log in.
D. The threshold for locking out administrator accounts is too high, and it should be changed from five to three to prevent unauthorized access attempts.

Answer: A

QUESTION 1403
A developer is creating a new web application on a public cloud platform and wants to ensure the application can respond to increases in load while minimizing costs during periods of low usage. Which of the following strategies is MOST relevant to the use-case?

A. Elasticity
B. Redundancy
C. High availability
D. Non-persistence

Answer: A

QUESTION 1404
A tester was able to leverage a pass-the-hash attack during a recent penetration test. The tester gained a foothold and moved laterally through the network. Which of the following would prevent this type of attack from reoccurring?

A. Renaming all active service accounts and disabling all inactive service accounts
B. Creating separate accounts for privileged access that are not used to log on to local machines
C. Enabling full-disk encryption on all workstations that are used by administrators and disabling RDP

D. Increasing the password complexity requirements and setting account expiration dates

Answer: B

QUESTION 1405
A critical enterprise component whose loss or destruction would significantly impede business operations or have an outsized impact on corporate revenue is known as:

A. a single point of failure.
B. critical system infrastructure.
C. proprietary information.
D. a mission-essential function.

Answer: D

QUESTION 1406
A pass-the-hash attack is commonly used to:

A. modify DNS records to point to a different domain.
B. modify the IP address of the targeted computer.
C. execute java script to capture user credentials.
D. laterally move across the network.

Answer: D

QUESTION 1407
Which of the following enables a corporation to extend local security policies to corporate resources hosted in a CSP's infrastructure?

A. PKI
B. CRL
C. Directory services
D. CASB
E. VDI

Answer: D

QUESTION 1408
Which of the following is the main difference between symmetric and asymmetric cryptographic algorithms?

A. The use of PKI in symmetric algorithms
B. HSM-based key generation
C. Only one key used in symmetric algorithms
D. Random vs. pseudo-random key generation

Answer: C