- **Vendor: CompTIA**
- **Exam Code: SY0-601**
- **Exam Name: CompTIA Security+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in July/2021)**

QUESTION 400
A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess Its security.
Strategy for mitigating risks within the perimeter Which of the following solutions would BEST support the organization's strategy?

A. FIM
B. DLP
C. EDR
D. UTM

Answer: C

QUESTION 401
A security analyst b concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should he analyst monitor?

A. SFTP
B. AS
C. Tor
D. IoC

Answer: C

QUESTION 402
A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors'?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Answer: B

QUESTION 403
A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

Answer: B

QUESTION 404
n organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

Answer: C

QUESTION 405
A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

A. Installing WAPs with strategic placement
B. Configuring access using WPA3
C. Installing a WIDS
D. Enabling MAC filtering
E. Changing the WiFi password every 30 days
F. Reducing WiFi transmit power throughout the office

Answer: BD

QUESTION 406
A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:
- Employees must provide an alternate work location (i.e., a home address)
- Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?

A. Geofencing, content management, remote wipe, containerization, and storage segmentation
B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

QUESTION 407
A security administrator is analyzing the corporate wireless network The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports Which erf the following attacks in happening on the corporate network?

A. Man in the middle
B. Evil twin
C. Jamming
D. Rogue access point
E. Disassociation

Answer: B

QUESTION 408
During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1a
B. chflags
C. chmod
D. leof
E. setuid

Answer: D

QUESTION 409
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which of the following configuration should an analyst enable to improve security? (Select Two)

A. RADIUS
B. PEAP
C. WPS
D. WEP-TKIP
E. SSL
F. WPA2-PSK

Answer: DF

QUESTION 410
A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=../../../../../../../../../../etc/passwd
GET index.php?page=../../../../../../../../../../../etc/passwd
GET index.php?page=../../../../../../../../../../../../etc/passwd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal
B. SQL injection
C. API
D. Request forgery

Answer: D

QUESTION 411
The spread of misinformation surrounding the outbreak of a novel virus on election day ted to eligible voters choosing not to take the risk of going to the polls This is an example of:

A. prepending.

B. an influence campaign
C. a watering-hole attack
D. intimidation
E. information elicitation

Answer: D

QUESTION 412
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A split-tunnel VPN
D. Load-balanced servers

Answer: B

QUESTION 413
An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM
B. CASB
C. TPM
D. DLP

Answer: A

QUESTION 414
Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

A. Chain of custody
B. Checksums
C. Non-repudiation
D. Legal hold

Answer: A

QUESTION 415
The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3$"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity

D. Account lockout

Answer: D

QUESTION 416
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations
B. It provides insurance in case of a data breach
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance
E. It assures customers that the organization meets security standards

Answer: E

QUESTION 417
Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing

Answer: D

QUESTION 418
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT
B. Ransomware
C. Polymophic
D. A worm

Answer: C

QUESTION 419
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption

Answer: B

QUESTION 420
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: A

QUESTION 421
A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backups followed by differential backups

Answer: B

QUESTION 422
Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

QUESTION 423
Joe, an employee, is transferring departments and is providing copies of his files to a network share folder for his previous team to access. Joe is granting read-write-execute permissions to his manager but giving read-only access to the rest of the team. Which of the following access controls is Joe using?

A. FACL
B. DAC
C. ABAC
D. MAC

Answer: D

QUESTION 424
When implementing automation with loT devices, which of the following should be considered FIRST to keep the network secure?

A. 2-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

Answer: D