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

QUESTION 1180
A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:
- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.
Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

Answer: C

QUESTION 1181
During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive
B. RAM
C. Network attached storage
D. USB flash drive

Answer: B

QUESTION 1182
A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES
B. AES
C. MD5
D. RSA

Answer: C

QUESTION 1183
A mobile application developer wants to secure an application that transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling
B. Chaining
C. Signing
D. Pinning

Answer: D

QUESTION 1184
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

Answer: B

QUESTION 1185
A technician is designing a solution that will be required to process sensitive information, including classified government data. The system needs to be common criteria certified. Which of the following should the technician select?

A. Security baseline
B. Hybrid cloud solution
C. Open-source software applications
D. Trusted operating system

Answer: D

QUESTION 1186
While testing a new vulnerability scanner, a technician becomes concerned about reports that list security concerns that are not present on the systems being tested. Which of the following BEST describes this flaw?

A. False positives
B. Crossover error rate
C. Uncredentialed scan
D. Passive security controls

Answer: A

QUESTION 1187
An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

Answer: C

QUESTION 1188

During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to $20 million damages for the cost of $30,000 a year. Which of the following risk response techniques has the company chosen?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

Answer: A

QUESTION 1189
To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

Answer: D

QUESTION 1190
A security team has downloaded a public database of the largest collection of password dumps on the Internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list. Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration
D. Group policy, password history, password encryption

Answer: C

QUESTION 1191
A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Choose two.)

A. Use a unique managed service account.
B. Utilize a generic password for authenticating.
C. Enable and review account audit logs.
D. Enforce least possible privileges for the account.
E. Add the account to the local administrators group.
F. Use a guest account placed in a non-privileged users group.

Answer: AD

QUESTION 1192
An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures

B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

Answer: C

QUESTION 1193
A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attack?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

Answer: D

QUESTION 1194
Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.
B. The vulnerability scanner is able to inventory software on the target.
C. A scan will reveal data loss in real time.
D. Black-box testing can be performed.

Answer: B

QUESTION 1195
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. Onetime passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

Answer: C

QUESTION 1196
Which of the following would provide a safe environment for an application to access only the resources needed to function while not having access to run at the system level?

A. Sandbox
B. Honeypot
C. GPO
D. DMZ

Answer: A