Correct Answer: C

QUESTION 256
A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST these requirement?

A. RA
B. OCSP
C. CRL
D. CSR
Correct Answer: C
Explanation:
A CRL can still be preferred over the use of OCSP if a server has issued many certificates to be validated within a single revocation period. It may be more efficient for the organization to download a CRL at the beginning of the revocation period than to utilize the OCSP standard, necessitating an OCSP response every time a certificate requires validation.

QUESTION 257
Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

A. An SLA
B. An NDA
C. A BPA
D. An MOU

Correct Answer: D

QUESTION 258
Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

A. SOAR playbook
B. Security control matrix
C. Risk management framework
D. Benchmarks

Correct Answer: D

QUESTION 259
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported.

Correct Answer: A

QUESTION 260
A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN
B. Drive encryption
C. Network firewall
D. File level encryption
E. USB blocker
F. MFA

Correct Answer: BE

QUESTION 261
A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

A. Password and security question
B. Password and CAPTCHA
C. Password and smart card
D. Password and fingerprint
E. Password and one-time token
F. Password and voice

Correct Answer: CD

QUESTION 262
A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

A. Port
B. Intrusive
C. Host discovery
D. Credentialed

Correct Answer: D

QUESTION 263
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. data controller.
B. data owner
C. data custodian.
D. data processor

Correct Answer: D

QUESTION 264
To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS
B. IaaS
C. SaaS
D. PaaS

Correct Answer: D

QUESTION 265
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetworkd\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Correct Answer: D
Explanation:
"Brute force attack in which stolen user account names and passwords are tested against multiple websites." CompTIA SY0-601 Official Study Guide Page 690 This is a poorly worded question and while credential stuffing is a type of brute force attack, the information given does not indicate multiple websites. At best, this looks like a password spraying attack, but it is more likely a brute-force attack. Also note the output reads "unsername" and not "username" - perhaps irrelevant but the little things can and do matter

QUESTION 266
An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. Black-box
C. Gray-box
D. White-box
E. Red-team

Correct Answer: D
Explanation:
White box penetration testing, sometimes referred to as crystal or oblique box pen testing, involves sharing full network and system information with the tester, including network maps and credentials. This helps to save time and reduce the overall cost of an engagement https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/#:~:text=White%20box%20penetration%20testing%2C%20sometimes,including%20network%20maps%20and%20credentials.

QUESTION 267
A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rale
D. Attestation

Correct Answer: A
Explanation:
Where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

QUESTION 268
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

Correct Answer: B

QUESTION 269
Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

A. Testing security systems and processes regularly
B. Installing and maintaining a web proxy to protect cardholder data
C. Assigning a unique ID to each person with computer access
D. Encrypting transmission of cardholder data across private networks
E. Benchmarking security awareness training for contractors
F. Using vendor-supplied default passwords for system passwords

Correct Answer: AC
Explanation:
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

QUESTION 270
Which of the following attacks MOST likely occurred on the user's internal network?

- Name: Wikipedia.org
- Address: 208.80.154.224

A. DNS poisoning
B. URL redirection
C. ARP poisoning
D. /etc/hosts poisoning

Correct Answer: A

QUESTION 271
Which of the following would a European company interested in implementing a technical, hands-on set of security standards MOST likely choose?

A. GOPR
B. CIS controls
C. ISO 27001
D. ISO 37000

Correct Answer: A

QUESTION 272
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

A. Implement input validations
B. Deploy MFA
C. Utilize a WAF
D. Configure HIPS

Correct Answer: C

QUESTION 273
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD

Correct Answer: AD