A. Token key
B. Static code
C. Push notification
D. HOTP

Correct Answer: A

QUESTION 311
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key

Correct Answer: B
Explanation:
While key size is probably the most important factor its not the only factor. "length of time" is basically interchangeable with the term longevity. "Longevity depends upon the robustness of the algorithm, a long key length (i.e., large key space), random key selection, and reliable key management over the desired protection timeframe. The longer a key is in use or the more often the same key is used, the higher the probability that it could be compromised. When a symmetric key is used to encrypt an entire storage device [i.e., full-disk encryption (FDE)], that key may be static for years. When a public key pair set is issued or defined, it is often used for a year before being replaced. These conditions require solid algorithms and long keys to counterbalance the risk of long-term use or repeated use."

QUESTION 312
Which of the following is the correct order of volatility from MOST to LEAST volatile?

A. Memory, temporary filesystems, routing tables, disk, network storage
B. Cache, memory, temporary filesystems, disk, archival media
C. Memory, disk, temporary filesystems, cache, archival media
D. Cache, disk, temporary filesystems, network storage, archival media

Correct Answer: B

QUESTION 313
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related
to:

A. whaling.
B. smishing.
C. spear phishing
D. vishing

Correct Answer: C

QUESTION 314
A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

- Must be able to differentiate between users connected to WiFi
- The encryption keys need to change routinely without interrupting the users or forcing reauthentication
- Must be able to integrate with RADIUS
- Must not have any open SSIDs

Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise
B. WPA3-PSK
C. 802.11n
D. WPS

Correct Answer: C

QUESTION 315
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
Correct Answer: A
Explanation:
A hardware security module (HSM) is a security device you can add to a system to manage, generate, and securely store cryptographic keys.

High performance HSMs are external devices connected to a network using TCP/IP. Smaller HSMs come as expansion cards you install within a server, or as devices you plug into computer ports.

QUESTION 316
A security researcher is attempting to gather data on the widespread use of a Zero-day exploit. Which of the following will the researcher MOST likely use to capture this data?

A. A DNS sinkhole
B. A honeypot
C. A vulnerability scan
D. CVSS

Correct Answer: B

QUESTION 317
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

Correct Answer: C

QUESTION 318
The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots It uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

A. Baseline modification
B. A fileless virus
C. Tainted training data
D. Cryptographic manipulation

Correct Answer: C

QUESTION 319
An administrator is experiencing issues when trying to upload a support file to a vendor. A pop-up message reveals that a payment card number was found in the file, and the file upload was blocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

A. DLP
B. Firewall rule
C. Content filter
D. MDM
E. Application whitelist

Correct Answer: A

QUESTION 320
A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help to accomplish this goal?

A. Classify the data
B. Mask the data
C. Assign the application owner
D. Perform a risk analysis

Correct Answer: A

QUESTION 321

An organization has hired a red team to simulate attacks on its security posture. Which of the following will the blue team do after detecting an IoC?

A. Reimage the impacted workstations.
B. Activate runbooks for incident response
C. Conduct forensics on the compromised system
D. Conduct passive reconnaissance to gather information

Correct Answer: C

QUESTION 322
The website http://companywebsite.com requires users to provide personal information including security responses, for registration. Which of the following would MOST likely cause a date breach?

A. Lack of input validation
B. Open permissions
C. Unsecure protocol
D. Missing patches

Correct Answer: C

QUESTION 323
A user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is fully patched. The user downloaded a driver package from the internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is MOST likely cause of the infection?

A. The driver has malware installed and was refactored upon download to avoid detection.
B. The user's computer has a rootkit installed that has avoided detection until the new driver overwrote key files.
C. The user's antivirus software definition were out of date and were damaged by the installation of the driver
D. The user's computer has been infected with a logic bomb set to run when new driver was installed.

Correct Answer: A

QUESTION 324
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

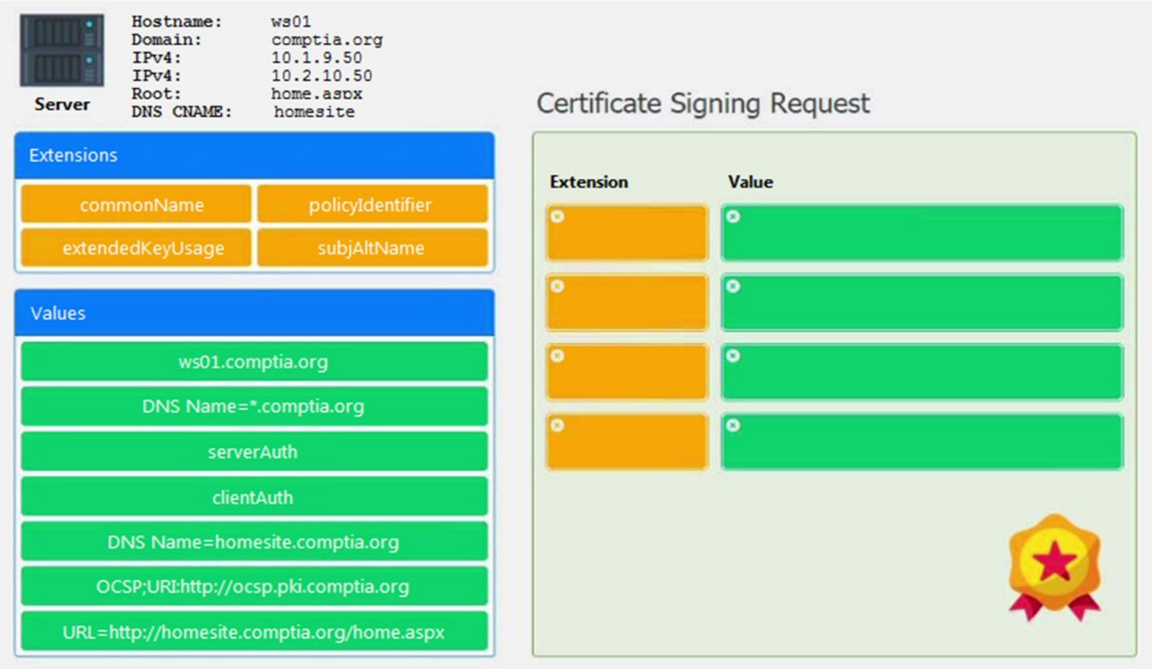
Correct Answer: A

QUESTION 325
DRAG DROP
Leveraging the information supplied below, complete the CSR for the server to set up TLS

(HTTPS)

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPV4: 10.2.10.50
- Root: home.aspx
- DNS CNAME:homesite.

Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.



Server

```
Hostname:     ws01
Domain:       comptia.org
IPv4:         10.1.9.50
IPv4:         10.2.10.50
Root:         home.aspx
DNS CNAME:    homesite
```

Extensions

- commonName
- policyIdentifier
- extendedKeyUsage
- subjAltName

Values

- ws01.comptia.org
- DNS Name=*.comptia.org
- serverAuth
- clientAuth
- DNS Name=homesite.comptia.org
- OCSP;URI:http://ocsp.pki.comptia.org
- URL=http://homesite.comptia.org/home.aspx

Certificate Signing Request

Extension	Value

Correct Answer: