

- 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 is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the 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 data 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 left 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:



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
commonName	ws01.comptia.org
extendedKeyUsage	OCSP;URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homesite.comptia.org/home.aspx
subjAltName	DNS Name=*.comptia.org



QUESTION 326

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

- A. Pass-the-hash
- B. Brute-force
- C. Directory traversal
- D. Replay

Correct Answer: A

QUESTION 327

An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model. Which of the following BEST describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols
- C. Default settings
- D. Open permissions

Correct Answer: C

QUESTION 328

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

Correct Answer: C

QUESTION 329

An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to