

[Download Full Version JK0-022 Exam Dumps\(Updated in Feb/2023\)](#)

to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

Correct Answer: A

Explanation:

<https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/>

QUESTION 26

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

Correct Answer: D

QUESTION 27

Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

- A. A worm that has propagated itself across the intranet, which was initiated by presentation media
- B. A fileless virus that is contained on a vCard that is attempting to execute an attack
- C. A Trojan that has passed through and executed malicious code on the hosts
- D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Correct Answer: A

QUESTION 28

Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

- A. Spear phishing
- B. Whaling
- C. Phishing
- D. Vishing

Correct Answer: C

Explanation:

<https://en.wikipedia.org/wiki/Phishing>

QUESTION 29

A network administrator needs to build out a new datacenter, with a focus on resiliency and

[JK0-022 Exam Dumps](#) **[JK0-022 PDF Dumps](#)** **[JK0-022 VCE Dumps](#)** **[JK0-022 Q&As](#)**

<https://www.ensurepass.com/JK0-022.html>

uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

Correct Answer: AB

Explanation:

<https://searchdatacenter.techtarget.com/definition/resiliency>

QUESTION 30

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

Correct Answer: A

QUESTION 31

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

Correct Answer: C

Explanation:

Dump files are a special type of files that store information about your computer, the software on it, and the data loaded in the memory when something bad happens. They are usually automatically generated by Windows or by the apps that crash, but you can also manually generate them.

<https://www.digitalcitizen.life/view-contents-dump-file/>

QUESTION 32

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

Correct Answer: C

QUESTION 33

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

Correct Answer: A

QUESTION 34

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation, a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP.
- The forged website's IP address appears to be 10.2.12.99, based on NetFlow records.
- AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP.
- DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

- A. A reverse proxy was used to redirect network traffic
- B. An SSL strip MITM attack was performed
- C. An attacker temporarily pawned a name server
- D. An ARP poisoning attack was successfully executed

Correct Answer: B

QUESTION 35

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes. Which of the following is the 60-minute expectation an example of:

- A. MTBF
- B. RPO
- C. MTTR
- D. RTO

Correct Answer: D

Explanation:

<https://www.enterprisestorageforum.com/management/rpo-and-rto-understanding-the-differences/>

QUESTION 36

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of

[JK0-022 Exam Dumps](#) [JK0-022 PDF Dumps](#) [JK0-022 VCE Dumps](#) [JK0-022 Q&As](#)

<https://www.ensurepass.com/JK0-022.html>

[Download Full Version JK0-022 Exam Dumps\(Updated in Feb/2023\)](#)

the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

Correct Answer: B

QUESTION 37

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

- A. Rainbow table
- B. Brute-force
- C. Password-spraying
- D. Dictionary

Correct Answer: C

Explanation:

Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

<https://us-cert.cisa.gov/ncas/current-activity/2019/08/08/acsc-releases-advisory-password-spraying-attacks#:~:text=Password%20spraying%20is%20a%20type,rapid%20or%20frequent%20account%20lockouts.>

QUESTION 38

A security analyst has received an alert about being sent via email. The analyst's Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care. From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP
- D. HIDS

Correct Answer: B

Explanation:

Network-based DLP monitors outgoing data looking for sensitive data. Network-based DLP systems monitor outgoing email to detect and block unauthorized data transfers and monitor data stored in the cloud.

[JK0-022 Exam Dumps](#) [JK0-022 PDF Dumps](#) [JK0-022 VCE Dumps](#) [JK0-022 Q&As](#)

<https://www.ensurepass.com/JK0-022.html>

QUESTION 39

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

Correct Answer: B

QUESTION 40

A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

- A. Salting the magnetic strip information
- B. Encrypting the credit card information in transit.
- C. Hashing the credit card numbers upon entry.
- D. Tokenizing the credit cards in the database

Correct Answer: C

QUESTION 41

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Correct Answer: D

QUESTION 42

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

Correct Answer: B