

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

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is MOST likely the cause?

- A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
- B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
- C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
- D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Correct Answer: D

QUESTION 359

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

- A. ISO 27701
- B. The Center for Internet Security
- C. SSAE SOC 2
- D. NIST Risk Management Framework

Correct Answer: D

QUESTION 360

A security analyst has been asked by the Chief Information Security Officer to:

- develop a secure method of providing centralized management of infrastructure
- reduce the need to constantly replace aging end user machines
- provide a consistent user desktop experience

Which of the following BEST meets these requirements?

- A. BYOD
- B. Mobile device management
- C. VDI
- D. Containerization

Correct Answer: B

QUESTION 361

To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?

- A. Install a hypervisor firewall to filter east-west traffic.
- B. Add more VLANs to the hypervisor network switches.
- C. Move exposed or vulnerable VMs to the DMZ.
- D. Implement a zero-trust policy and physically segregate the hypervisor servers.

Correct Answer: B

QUESTION 362

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 363

A website developer who is concerned about theft of the company's user database warns to protect weak passwords from offline brute-force attacks. Which of the following be the BEST solution?

- A. Lock accounts after five failed logons
- B. Precompute passwords with rainbow tables
- C. Use a key-stretching technique
- D. Hash passwords with the MD5 algorithm

Correct Answer: A

QUESTION 364

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

- A. WEP
- B. MSCHAP
- C. WPS
- D. SAE

Correct Answer: D

Explanation:

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.[3][4] The new standard uses 128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise)[5] and forward secrecy.[6] The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode
https://en.wikipedia.org/wiki/Simultaneous_Authentication_of_Equals#:~:text=In%20cryptography%2C%20Simultaneous%20Authentication%20of,password%2Dauthenticated%20key%20agreement%20method.

QUESTION 365

Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

Correct Answer: D

QUESTION 366

Which of the following types of attacks is being attempted and how can it be mitigated?

<http://comptia.org/ ../ ../etc/passwd>

- A. XSS; implement a SIEM
- B. CSRF; implement an IPS
- C. Directory traversal: implement a WAF
- D. SQL injection: implement an IDS

Correct Answer: C

QUESTION 367

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?

- A. Functional testing
- B. Stored procedures
- C. Elasticity
- D. Continuous integration

Correct Answer: D

Explanation:

[https://www.cloudbees.com/continuous-delivery/continuous-integration#:~:text=Continuous%20Integration%20\(CI\)%20is%20a,automated%20build%20and%20automated%20tests](https://www.cloudbees.com/continuous-delivery/continuous-integration#:~:text=Continuous%20Integration%20(CI)%20is%20a,automated%20build%20and%20automated%20tests).

Continuous Integration (CI) is a development practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration can then be verified by an automated build and automated tests.

QUESTION 368

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

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

Correct Answer: C

QUESTION 369

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

- A. Key escrow
- B. A self-signed certificate
- C. Certificate chaining
- D. An extended validation certificate

Correct Answer: B

QUESTION 370

A developer is concerned about people downloading fake malware-infected replicas of a popular game. Which of the following should the developer do to help verify legitimate versions of the game for users?

- A. Digitally sign the relevant game files.
- B. Embed a watermark using steganography.
- C. Implement TLS on the license activation server.
- D. Fuzz the application for unknown vulnerabilities.

Correct Answer: A

Explanation:

[https://us-cert.cisa.gov/ncas/tips/ST04-](https://us-cert.cisa.gov/ncas/tips/ST04-018#:~:text=A%20digital%20signature%E2%80%94type,%2C%20or%20a%20digital%20document).)

[018#:~:text=A%20digital%20signature%E2%80%94type,%2C%20or%20a%20digital%20document\).](https://us-cert.cisa.gov/ncas/tips/ST04-018#:~:text=A%20digital%20signature%E2%80%94type,%2C%20or%20a%20digital%20document).)

<https://www.techtarget.com/searchsecurity/definition/digital-signature>

QUESTION 371

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

Correct Answer: C

QUESTION 372

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A reverse proxy
- B. A decryption certificate

- C. A split-tunnel VPN
- D. Load-balanced servers

Correct Answer: A

QUESTION 373

HOTSPOT

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS:

Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions:

The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

Network Diagram

