

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

QUESTION 100

DRAG DROP

A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	
<code>chmod 777 ~/.ssh/authorized_keys</code>	
<code>ssh-keygen -t rsa</code>	
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

Correct Answer:

Commands	SSH Client
<code>chmod 644 ~/.ssh/id_rsa</code>	<code>ssh-keygen -t rsa</code>
<code>chmod 777 ~/.ssh/authorized_keys</code>	<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>
<code>ssh-keygen -t rsa</code>	<code>ssh -i ~/.ssh/id_rsa user@server</code>
<code>scp ~/.ssh/id_rsa user@server:~/.ssh/authorized_keys</code>	
<code>ssh-copy-id -i ~/.ssh/id_rsa.pub user@server</code>	
<code>ssh -i ~/.ssh/id_rsa user@server</code>	
<code>ssh root@server</code>	

QUESTION 101

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

Correct Answer: A

QUESTION 102

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected. Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)

- A. DoS
- B. SSL stripping
- C. Memory leak
- D. Race condition
- E. Shimming
- F. Refactoring

Correct Answer: AC

Explanation:

"According to its self-reported version, the Cisco IOS software running on the remote device is affected by a denial of service vulnerability in the Session Initiation Protocol (SIP) gateway implementation due to improper handling of malformed SIP messages. An unauthenticated, remote attacker can exploit this, via crafted SIP messages, to cause memory leakage, resulting in an eventual reload of the affected device."

QUESTION 103

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fireless virus is spreading in the local network environment.

Correct Answer: A

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

Explanation:

<https://www.howtogeek.com/362203/what-is-a-tar.gz-file-and-how-do-i-open-it/>

QUESTION 104

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

Correct Answer: D

QUESTION 105

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

Correct Answer: C

Explanation:

ISO 27701 also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy. Privacy information management systems are sometimes referred to as personal information management systems.

<https://pecb.com/whitepaper/the-future-of-privacy-with-isoiec-27701>

QUESTION 106

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

Correct Answer: C

Explanation:

<https://www.redlegg.com/solutions/advisory-services/tabletop-exercise-pretty-much-everything-you-need-to-know>

QUESTION 107

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

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

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

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

Correct Answer: D

Explanation:

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

QUESTION 108

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

Correct Answer: C

Explanation:

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

QUESTION 109

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Correct Answer: D

QUESTION 110

A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

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

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

Correct Answer: A

QUESTION 111

A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

- A. Trusted Platform Module
- B. A host-based firewall
- C. A DLP solution
- D. Full disk encryption
- E. A VPN
- F. Antivirus software

Correct Answer: AB

QUESTION 112

Which of the following describes the BEST approach for deploying application patches?

- A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
- B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems
- C. Test the patches in a test environment apply them to the production systems and then apply them to a staging environment
- D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Correct Answer: A

QUESTION 113

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

Correct Answer: A

QUESTION 114

Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

[JK0-022 Exam Dumps](#) **[JK0-022 PDF Dumps](#) **[JK0-022 VCE Dumps](#) **[JK0-022 Q&As](#)
<https://www.ensurepass.com/JK0-022.html>******