JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following offerings typically allows the customer to apply operating system patches?

A. Software as a service

B. Public Clouds

C. Cloud Based Storage

D. Infrastructure as a service

Correct Answer: D

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

Incorrect Answers:

A: In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.

B: A cloud is called a "public cloud" when the services are rendered over a network that is open for public use.

C: Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers, and the physical environment is typically owned and managed by a hosting company.

References: http://en.wikipedia.org/wiki/Cloud_computing http://en.wikipedia.org/wiki/Cloud_storage

QUESTION 2

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots

B. Sandboxing

C. Patch management

D. Intrusion detection system

Correct Answer: C

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

Incorrect Answers:

A: Snapshots are backups of virtual machines that can be used to quickly recover from errors or poor updates. It does

not ensure that the latest kernel version with all current security fixes is installed on the system.

B: Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

D: An intrusion detection system (IDS) is an automated system that detects intrusions or security policy violations on networks or host systems. It does not ensure that the latest kernel version with all current security fixes is installed on the system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 204-205, 220 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 21, 231-232, 249,

QUESTION 3

Which of the following can be used by a security administrator to successfully recover a user\\'s forgotten password on a password protected file?

A. Cognitive password

B. Password sniffing

C. Brute force

D. Social engineering

Correct Answer: C

One way to recover a user\\'s forgotten password on a password protected file is to guess it. A brute force attack is an automated attempt to open the file by using many different passwords.

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization\\'s network security. A brute force attack may also be referred to as brute force cracking. For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers. An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

Incorrect Answers:

A: A cognitive password is a form of knowledge-based authentication that requires a user to answer a question to verify their identity. To open the password protected file, we need the password that was used to protect the file. Therefore, this answer is incorrect.

B: Password sniffing is the process of capturing a password as it is transmitted over a network. As no one knows what the password for the protected file is, it won\\'t be transmitted over a network. Therefore, this answer is incorrect.

D: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. A social engineer runs what used to be called a

"con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network\\'s security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques. As no one knows what the password for the protected file is, we can\\'t use social engineering to reveal the password. Therefore, this answer is incorrect.

References:

http://www.techopedia.com/definition/18091/brute-force-attack http://searchsecurity.techtarget.com/definition/social-engineering

QUESTION 4

A security engineer is reviewing log data and sees the output below:

POST: /payload.php HTTP/1.1 HOST: localhost Accept: */* Referrer: http://localhost/ ******* HTTP/1.1 403 Forbidden Connection: close

Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

A. Host-based Intrusion Detection System

B. Web application firewall

C. Network-based Intrusion Detection System

D. Stateful Inspection Firewall

E. URL Content Filter

Correct Answer: B

A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It\\'s intended to be an application-specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks.

Incorrect Answers:

A: A host-based IDS (HIDS) watches the audit trails and log fi les of a host system. It\\'s reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

C: NIDS is reliable for detecting attacks directed against a host, whether they originate from an external source or are being perpetrated by a user locally logged in to the host.

D: A stateful inspection firewall is aware that any valid outbound communication will trigger a corresponding response or reply from the external entity.

E: URL filtering involves blocking websites (or sections of websites) based solely on the URL, restricting access to specified websites and certain web-based applications.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 19, 20, 21.

QUESTION 5

A small company wants to employ PKI. The company wants a cost effective solution that must be simple and trusted. They are considering two options: X.509 and PGP. Which of the following would be the BEST option?

A. PGP, because it employs a web-of-trust that is the most trusted form of PKI.

B. PGP, because it is simple to incorporate into a small environment.

C. X.509, because it uses a hierarchical design that is the most trusted form of PKI.

D. X.509, because it is simple to incorporate into a small environment.

Correct Answer: B