Accelerate Your Certification with CompTIA XK0-006 Practice Questions

Last chance to prepare smart! Get your hands on free CompTIA Linux+ V8 Exam PDF questions. Study real XK0-006 dumps with verified answers and fast-track your certification success with PrepBolt XK0-006 exam pdf questions and answers.

Thank you for Downloading XK0-006 exam PDF Demo

https://prepbolt.com/XK0-006.html

QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Question 1

Question Type: MultipleChoice

SIMULATION

Joe, a user, has taken a position previously held by Ann. As a systems administrator, you

need to archive all the files from Ann's home directory and extract them into Joe's home

directory.

INSTRUCTIONS

Within each tab, click on an object to form the appropriate commands. Command objects may only be used once, but the spacebar _ object may be used multiple times. Not all objects will be used.

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

Options:

A- See the solution in Explanation below

Answer:

A

Explanation:

Archive Tab -- Create the archive from Ann's home directory

Correct Command:

tar -cvf /tmp/ann.tar -C /home/ ann

Extract Tab -- Extract the archive into Joe's home directory

Correct Command:

tar -xvf /tmp/ann.tar -C /home/ joe

This performance-based question tests file archiving and restoration using tar, a core System Management skill in the CompTIA Linux+ V8 objectives. The task requires preserving Ann's files and placing them correctly into Joe's home directory.

Archive Phase Explanation

The goal of the first step is to archive Ann's entire home directory without embedding the full path (/home/ann) inside the archive. This is accomplished using the -C option.

Command breakdown:

tar archive utility

-c create an archive

-v verbose output (optional but allowed)

-f /tmp/ann.tar specifies the archive file

-C /home/ changes directory before archiving

ann archives the ann directory only

This results in a clean archive containing Ann's files without absolute paths, which is best practice and explicitly covered in Linux+ V8 documentation.

Extract Phase Explanation

The second step extracts the archived files into Joe's home directory.

Command breakdown:

-x extract

-v verbose

-f /tmp/ann.tar specifies the archive

-C /home/joe extracts files directly into Joe's home directory

This ensures Joe receives Ann's files correctly under /home/joe/ann or directly under /home/joe depending on post-extraction handling, which matches Linux+ expectations for administrative user transitions.

Question 2

Question Type: Hotspot

A junior system administrator removed an LVM volume by mistake.

INSTRUCTIONS

Part 1

Review the output and select the appropriate command to begin the recovery process.

Part 2

Review the output and select the appropriate command to continue the recovery process.

Part 3

Review the output and select the appropriate command to complete the recovery process and access the underlying data.

Answer:

See the Answer in the Premium Version!

Question 3

Question Type: Hotspot

A new drive was recently added to a Linux system. Using the environment and tokens provided, complete the following tasks:

* Create an appropriate device label.

* Format and create an ext4 file system on the new partition.

The current working directory is /.

Answer:

See the Answer in the Premium Version!

Question 4

Question Type: MultipleChoice

A systems administrator is configuring new Linux systems and needs to enable passwordless authentication between two of the servers. Which of the following commands should the administrator

use?

Options:

A- ssh-keygen -t rsa && ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2
B- ssh-keyscan -t rsa && ssh-copy-id john@server2 -i ~/.ssh/key
C- ssh-agent -i rsa && ssh-copy-id ~/.ssh/key john@server2
D- ssh-add -t rsa && scp -rp ~/.ssh john@server2

Answer:

A

Explanation:

Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:

Passwordless authentication using SSH key pairs is a foundational security practice covered in the Security domain of CompTIA Linux+ V8. It allows administrators to securely authenticate between systems without transmitting passwords over the network, significantly reducing the risk of credential compromise.

The correct approach involves two essential steps: generating an SSH key pair and installing the public key on the remote system. Option A correctly performs both steps using best-practice commands.

The command ssh-keygen -t rsa generates an RSA public/private key pair in the user's ~/.ssh/ directory. The private key (id_rsa) remains securely on the local system, while the public key (id_rsa.pub) is intended to be shared. The second part of the command, ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2, securely copies the public key to the remote server's ~/.ssh/authorized_keys file. This enables key-based authentication for the specified user.

The other options are incorrect or incomplete. Option B uses ssh-keyscan, which is intended for collecting host keys to populate known_hosts, not for user authentication. Option C misuses ssh-agent, which manages keys already generated and does not create or install them. Option D is insecure and incorrect because copying the entire .ssh directory risks exposing private keys and violates security best practices.

Linux+ V8 documentation emphasizes the use of ssh-keygen and ssh-copy-id as the standard, secure method for configuring passwordless SSH access. This approach ensures proper permissions, correct key placement, and minimal risk.

Question 5

Question Type: MultipleChoice

Which of the following passwords is the most complex?

Options:

A- H3sa1dt01d
B- he$@ID$heTold
C- H3s@1dSh3t0|d
D- HeSaidShetold

Answer:

C

Explanation:

Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:

Password complexity is a fundamental concept within the Security domain of CompTIA Linux+ V8. Complex passwords significantly reduce the risk of successful brute-force, dictionary, and credential-stuffing attacks. Linux+ emphasizes evaluating passwords based on length, character variety, unpredictability, and resistance to common word patterns.

Option C, H3s@1dSh3t0|d, is the most complex password among the choices. It demonstrates strong security characteristics by incorporating:

Uppercase letters (H, S)

Lowercase letters (s, d, t)

Numbers (3, 1, 0)

Multiple special characters (@, |)

A longer overall length compared to some other options

Additionally, option C uses character substitution (leet-style) in a way that breaks up recognizable words more effectively than the other choices. This significantly increases entropy and makes the password harder to guess using rule-based or hybrid cracking techniques.

Option A includes uppercase letters and numbers but lacks special characters and is relatively short. Option B includes special characters and mixed case, but it still closely resembles readable words, making it more susceptible to dictionary-based attacks. Option D uses only alphabetic characters and clear word patterns, making it the weakest choice.

Linux+ V8 documentation highlights that the strongest passwords combine length with diverse character classes and minimal predictability. Password C best meets all of these criteria and would score highest against common password-cracking strategies.

Therefore, the correct answer is C. H3s@1dSh3t0|d.

Thank You for trying XK0-006 PDF Demo

To try our XK0-006 practice exam software visit link below

https://prepbolt.com/XK0-006.html

Start Your XK0-006 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your XK0-006 preparation with actual exam questions.