SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.pass2lead.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

DRAG DROP

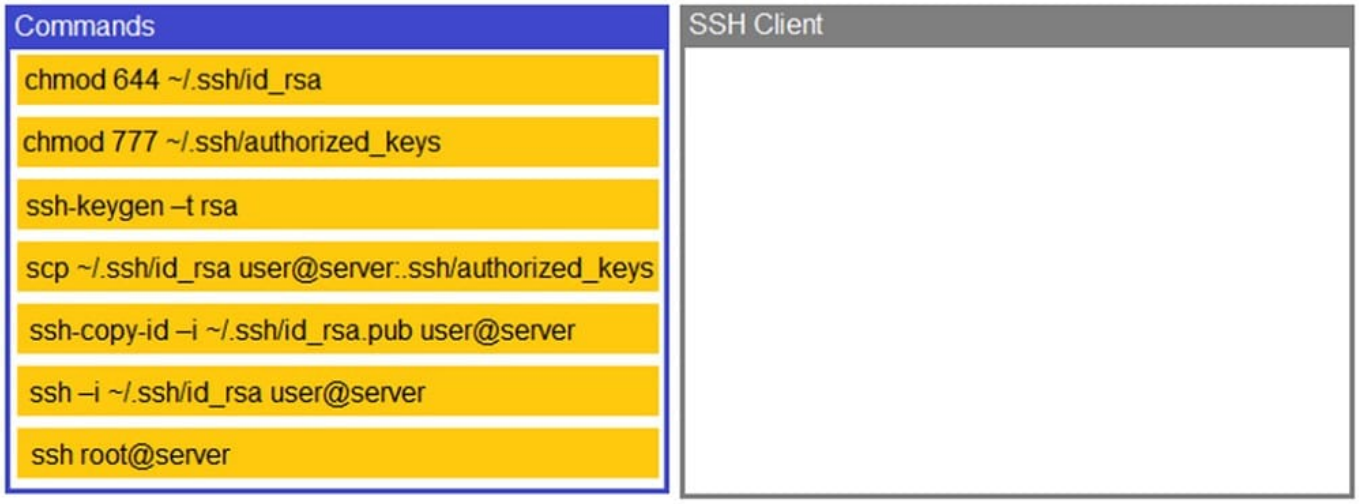
A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

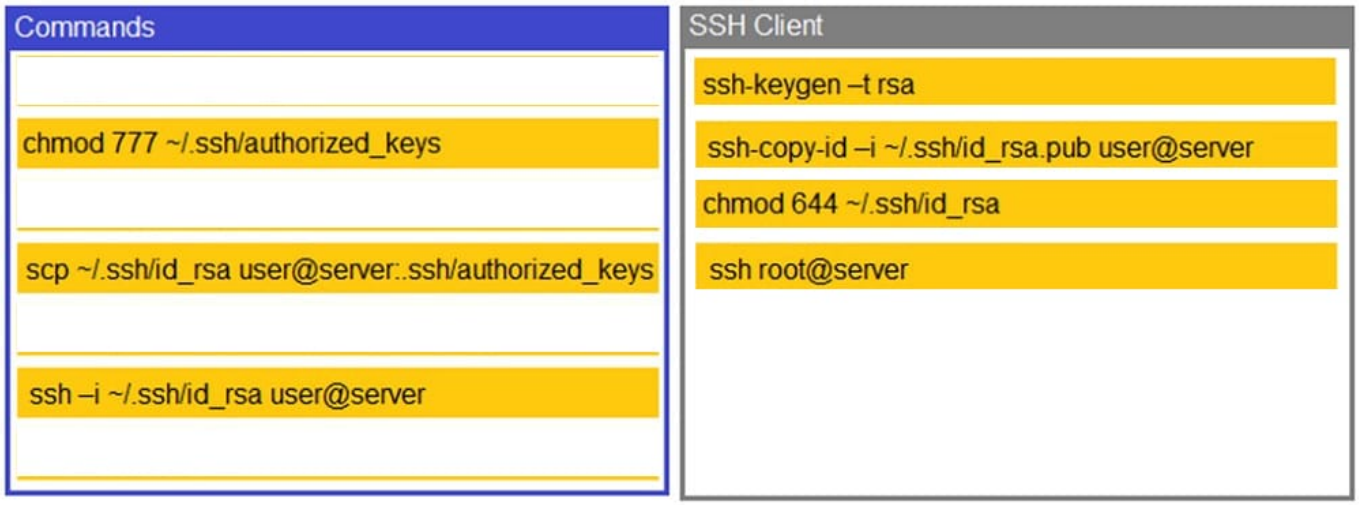
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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

Select and Place:



Correct Answer:



QUESTION 2

An application owner has requested access for an external application to upload data from the central internal website without providing credentials at any point. Which of the following authentication methods should be configured to allow this type of integration access?

A. OAuth

B. SSO

C. TACACS+

D. Kerberos

Correct Answer: B

QUESTION 3

A security operations analyst is using the company\\'s SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradication

B. Recovery

C. Identification

D. Preparation

Correct Answer: C

C: Identification

Incident response lifecycle:

-preparation

-detection and analysis

-containment, eradication, recovery

-post-incident activity

QUESTION 4

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT

B. Credential stuffing

C. SQL injection

D. Man in the browser

E. Bluejacking

Correct Answer: A

Another example of unintentional insider threat is the concept of shadow IT, where users purchase or introduce computer hardware or software to the workplace without the sanction of the IT department and without going through a procurement and security analysis process. The problem of shadow IT is exacerbated by the proliferation of cloud services and mobile devices, which are easy for users to obtain. Shadow IT creates a new unmonitored attack surface for malicious adversaries to exploit.

While SQL Injection might be one way that enterprise data from the local database was compromised, an attacker could simple have hacked into the person machine and opened up the local database to steal the data. SQL Injection is possible, but is not MOST Likely. You need to ask the question: If the enterprise has moved everything into the cloud, then the only reason there is a local database on the person\\'s machine is because they installed the database. They installed an application on their local machine when they should have been using an application on the company\\'s cloud. That, in its definition, is shadow IT.

QUESTION 5

he SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team

B. The vulnerability management team

C. The CIRT

D. The red team

Correct Answer: C

its CIRT Also known as a "computer incident response team," this group is responsible for responding to security breaches, viruses and other potentially catastrophic events . The NOC is network operations center , a centralized location where IT teams can continuously monitor the performance and health of a network(far away form incident responce