***Two entries associated now –***

***id\_rsa is the private key.***

***id\_rsa.pub is the public key.***

***Provide a screen shot of the result***.

A screenshot of a computer

Description automatically generated

***Provide a screen shot of the result of your public key***



***At this point you will receive a challenge like the one below.***

***7. Provide your passphrase that you used when you created the key.***

***8. Ip ad.***

***Provide a screen shot of the result***.

A white text with black text

Description automatically generated

***Now login to your client device. Execute –***

***11. cd .ssh***

***12. cat id\_rsa***

***13. cat id\_rsa.pub Provide a screenshot for submission.***

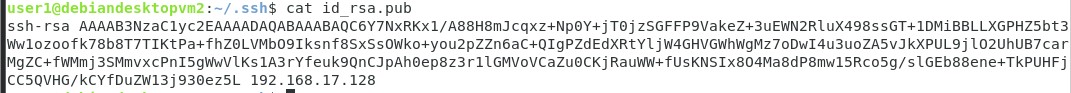
A close-up of a computer code

Description automatically generated

***Provide a screenshot for submission of the results of steps 11,12,13 from the server side (VMSVR1)***

A screenshot of a computer

Description automatically generated



A close up of a text

Description automatically generated

A close-up of a computer screen

Description automatically generated

Reflection Questions

1. How can the use of file encryption help protect an organization’s sensitive files? ***File encryption ensures sensitive data remains unreadable to unauthorized users***

2. What is the purpose of the passphrase when ssh-keygen was utilized? ***The passphrase encrypts the private key, adding an extra layer of security***

3. What is my security exposure if I do not use a passphrase? ***Without a passphrase, anyone with access to your private key can use it to gain unauthorized access to systems that trust the key***