15.10.4 Practice Questions

Candidate: Ethan Bonavida (suborange)
Date: 12/9/2022 12:37:35 am • **Time Spent:** 00:46

Score: 80% Passing Score: 80%

Question 1: ✕ Incorrect

What is the name of the hash function used to verify the public key for an SSH connection?

[ ] MD5

Explanation

MD5 is an algorithm intended for digital signature applications. MD5 is available on many operating systems, including Windows and Linux.

References

15.10.3 Public Key Authentication Facts

q_public_key_auth_f_lp5_01.question.fex

Question 2: ✔ Correct

Which keys are generated when you execute the **ssh-keygen** command with no options? (Select TWO.)

- [x] id_rsa
- [ ] id_dsa.pub
- [ ] id_dsa
- [x] id_rsa.pub

Explanation

Use **ssh-keygen** to create a key on the client for use when authenticating to a server. Be aware of the following **ssh-keygen** options:

- -**t dsa** creates a DSA key pair (i.e., id_dsa and id_dsa.pub).
- **-t rsa** creates an RSA key pair (i.e., id_rsa and id_rsa.pub). This action is also the default when no options are included.

The client uses the public and private key pairs to authenticate to the server.

References

15.10.3 Public Key Authentication Facts

q_public_key_auth_f_lp5_02.question.fex

Question 3: ✔ Correct

As you configure your client for public key authentication, you decide to generate the DSA key pair.

You would like to configure the client to automatically provide the private key passphrase when needed so that you do not need to type the passphrase for every new SSH connection to a server.

Which command should you use in conjunction with the ssh-agent bash command? (Enter the command and options as if you are at the command prompt.)

ssh-add ~/.ssh/id_dsa ✔

Explanation

Use **ssh-add ~/.ssh/id_dsa** to specify the name of the private key to add to the passphrase agent (either id_rsa or id_dsa).

Use **ssh-agent bash** and **ssh-add** to configure the client to automatically provide the private key passphrase when needed so that it does not have to be typed for every new connection to a server.

1. Use **ssh-agent bash** to enable the passphrase agent.
2. Use **ssh-add** to specify the name of the private key to add to the agent. For protocol 2, this is one of the following:
   - **~/.ssh/id_rsa**
   - **~/.ssh/id_dsa**

References

15.10.3 Public Key Authentication Facts

q_public_key_auth_f_lp5_03.question.fex

Question 4: ✔ Correct

You are configuring public key authentication on your client system. Which command enables the passphrase agent?

- **ssh-agent bash**
- **scp**
- **ssh-keygen**
- **ssh-add**

Explanation

ssh-agent bash enables the passphrase agent. Then you use **ssh-add** to specify the name of the private key to add to the agent (either id_rsa or id_dsa).

ssh-keygen creates a key on the client for use when authenticating to a server. **scp** encrypts and copies files from a remote system over the network.

References

15.10.3 Public Key Authentication Facts

q_public_key_auth_f_lp5_04.question.fex

Question 5: ✔ Correct

You want to enable public key authentication on the server. Which option in the /etc/ssh/sshd_config file needs to be set?

- #RSAAuthentication yes
- RSAAuthentication yes
- PubkeyAuthentication yes
- #PubkeyAuthentication yes

Explanation

The *PubkeyAuthentication* option in the /etc/ssh/sshd_config file is used to enable or disable public key authentication on the server. To enable public key authentication on the server, the option must be set to *PubkeyAuthentication yes*.

References

15.10.3 Public Key Authentication Facts

q_public_key_auth_f_lp5_05.question.fex