15.6.7 Practice Questions

Candidate: Ethan Bonavida (suborange)
Date: 12/9/2022 12:23:45 am • **Time Spent:** 02:00

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

Which is the most correct description for 3DES?

- 3DES is a third-generation version of DES, the Data Encryption Standard cipher.
- 3DES is derived from Microsoft's Windows Encrypted File System (EFS).
- ➡ 3DES is a very secure mode of the DES algorithm encryption method that encrypts data three times using a 168-bit key.
- 3DES means running the DES algorithm three times for maximum encryption.

Explanation

3DES is a secure mode of the DES algorithm that encrypts data with three different 56-bit keys in three different encryption passes (for a total of 168 key bits). 3DES is not derived from Microsoft's EFS. Running a DES algorithm three times is not the same as 3DES. 3DES does not mean it is the third generation of DES.

References

15.12.1 Security Best Practices

15.12.2 Security Best Practices Facts

q_encrypt_type_stand_lp5_01.question.fex

Question 2: ✔ Correct

Which version of SSH supports the Rivest, Shamir Adleman (RSA), and Digital Signature Algorithm (DSA) encryption standards?

SSH2 ✔

Explanation

SSH version 2 (SSH2) is the current standard SSH implementation. It can use either DSA or RSA encryption. SSH:

- Uses a public and private key pair to encode and transfer a symmetric key that is used during the session. The public key is available to all users. The private key is only available on the server and is never shared.
- Can use associated key management software and scripts to automate the exchange of public keys.
- Allows encryption of other network protocols, such as the X server protocols.

References

1.1.4 Server Roles Facts

15.6.1 OpenSSH

q_encryptf_lp5_01.question.fex

Question 3: ✔ Correct

Which of the following public keys is sent from the SSH server to the SSH client when they are in the process of establishing a session with the SSH1 protocol?

- **ssh_host_rsa_key.pub**
- **ssh_host_dsa_key.pub**
- **ssh_key.pub**
- **ssh_host_key.pub**

Explanation

The server sends the **ssh_host_key.pub** from the **/etc/ssh/** directory to the client in the process of establishing a session with the SSH1 protocol.

Computers use the following steps when establishing a session using SSH:

1. A client running SSH establishes a connection to the server (any computer running the SSH daemon) over port 22.
2. The computers determine which SSH version to use based on the specifications in the configuration files. Typically, SSH2 is used.
3. The server sends one of the following public keys from the **/etc/ssh/** directory to the client:
   - **ssh_host_key.pub** (SSH1 public key)
   - **ssh_host_rsa_key.pub** (SSH2 public key when using RSA)
   - **ssh_host_dsa_key.pub** (SSH2 public key when using DSA)
4. When the client receives the public key from the server, it compares the key to the keys it has received and stored in one of the following files:
   - **/etc/ssh/ssh_known_hosts**
   - **~/.ssh/known_hosts**

   If the key is not present in either of these files, the client prompts the user to accept and store the key.
5. The server and the client then use the Diffie-Hellman key exchange system to agree on a symmetric key that they use for the rest of the session.
6. The data is exchanged with symmetric encryption.

References

15.6.3 OpenSSH Facts

q_encryptf_lp5_02.question.fex

Question 4: ✔ Correct

Where does the client store SSH keys that are used to establish an SSH session? (Select TWO).

- [x] **~/.ssh/known_hosts**
- [x] **/etc/ssh/ssh_known_hosts**
- [ ] **~/.ssh/config**
- [ ] **/etc/ssh/sshd_config**

Explanation

When the client receives the public key from the SSH server, it compares the key to the keys it has received and stored in one of the following files:

- **/etc/ssh/ssh_known_hosts**
- **~/.ssh/known_hosts**

Use **/etc/ssh/sshd_config** to configure the SSH daemon on the server system. Use **~/.ssh/config** or **/etc/ssh/ssh_config** to configure the SSH daemon on the client system.

Computers use the following steps when establishing a session using SSH:

1. A client running SSH establishes a connection to the server (any computer running SSH daemon)) over port 22.
2. The computers determine which SSH version to use based on the specifications in the configuration files. Typically, SSH2 is used.
3. The server sends one of the following public keys from the **/etc/ssh/** directory to the client:
   - **ssh_host_key.pub** (SSH1 public key)
   - **ssh_host_rsa_key.pub** (SSH2 public key when using RSA)
   - **ssh_host_dsa_key.pub** (SSH2 public key when using DSA)
4. When the client receives the public key from the server, it compares the key to the keys it has received and stored in one of the following files:
   - **/etc/ssh/ssh_known_hosts**
   - **~/.ssh/known_hosts**

   If the key is not present in either of these files, the client prompts the user to accept and store the key.
5. The server and the client then use the Diffie-Hellman key exchange system to agree on a symmetric key that they use for the rest of the session.
6. The data is exchanged with symmetric encryption.

References

15.6.3 OpenSSH Facts

q_encryptf_lp5_03.question.fex

Question 5: ✔ Correct

When using DSA to establish an SSH session, what is the name of the key that the SSH server will send to the client? (Enter the name of the key only.)

ssh_host_dsa_key.pub ✔

Explanation

The server sends the **ssh_host_dsa_key.pub** from the **/etc/ssh/** directory to the client in the process of establishing a session when using DSA (Digital Signature Algorithm).

Computers use the following steps when establishing a session using SSH:

1. A client running SSH establishes a connection to the server (any computer running SSH daemon) over port 22.
2. The computers determine which SSH version to use based on the specifications in the configuration files. Typically, SSH2 is used.
3. The server sends one of the following public keys from the **/etc/ssh/** directory to the client:
   - **ssh_host_key.pub** (SSH1 public key)
   - **ssh_host_rsa_key.pub** (SSH2 public key when using RSA)
   - **ssh_host_dsa_key.pub** (SSH2 public key when using DSA)
4. When the client receives the public key from the server, it compares the key to the keys it has received and stored in one of the following files:
   - **/etc/ssh/ssh_known_hosts**
   - **~/.ssh/known_hosts**

   If the key is not present in either of these files, then the client prompts the user to accept and store the key.
5. The server and the client then use the Diffie-Hellman key exchange system to agree on a symmetric key that they use for the rest of the session.
6. The data is exchanged with symmetric encryption.

References

15.6.3 OpenSSH Facts

q_encryptf_lp5_04.question.fex

Question 6: ✔ Correct

You need to connect to a remote system whose host name is *abc.def.com* and execute a shell script called *daily-backup.sh* that backs up some files. The username that has permissions to execute that script is *bubba*.

Which command should you run to make the connection?

- **ssh -l bubba abc.def.com**
- **netstat abc.def.com bubba**
- **ssh abc.def.com:bubba**
- **ping abc.def.com:bubba**

Explanation

Use the **ssh** utility to connect to the remote host using a secure shell connection. Use the **-l** option to specify a name to use to make the connection. The only other variable you must give is the name of the host you want to connect with.

Use the **netstat** utility to see the status of sockets and related networking statistics. Use the **ping** utility to see if a host is reachable.

References

15.6.6 OpenSSH Configuration Facts

q_openssh_c_lp5_01.question.fex

Question 7: ✔ Correct

The *gshant* user is attempting to connect to a remote SSH server; however, you need to override the default SSH configurations for the client system when he establishes an SSH session.

Which of the following files should you edit?

- **/etc/ssh/ssh_known_hosts**
- **/etc/ssh/sshd_config**
- **/home/gshant/.ssh/config**
- **/etc/ssh/ssh_config**

Explanation

~/.ssh/config is a user-specific hidden file that can override the configuration in **/etc/ssh/ssh_config** file. The **/etc/ssh/ssh_config** file configures OpenSSH for all users on the client system.

The **/etc/ssh/sshd_config** file configures the SSH daemon on the server system. The client stores the public keys it receives from the server in one of the following files:

- **/etc/ssh/ssh_known_hosts**
- **~/.ssh/known_hosts**

References

15.6.6 OpenSSH Configuration Facts

q_openssh_c_lp5_02.question.fex

Question 8: ✔ Correct

You want to change the port that SSH listens on. You are going to edit the /etc/ssh/sshd_config file.

Which line, when added to the file, will change the listening port to 1066?

- ssh_port 1066
- listen_port 1066
- listen 1066
- ➡ port 1066

Explanation

The correct line is port 1066. The default port for ssh is 22, and changing it to 1066 adds additional security to your system. For example, to ssh into foobar.com, which is listening on port 1066, you would type the following command:

ssh -p 1066 root@foobar.com

The keywords listen, listen_port, and ssh_port are incorrect.

References

15.12.1 Security Best Practices

15.12.2 Security Best Practices Facts

q_openssh_c_lp5_03.question.fex

Question 9: ✔ Correct

A number of remote users call to say that they cannot connect via SSH today. When you look at the processes, you see that the daemon is not running.

Which command would you use to solve this problem?

- **inetd ssh**
- **ssh start**
- **/etc/inetd/ssh start**
- **/etc/rc.d/init.d/sshd start**

Explanation

The script controlling the ssh daemon resides in the /etc/rc.d/init.d directory and can be started with the **start** command.

References

15.4.2 Remove Unneeded Services and Scan Ports

q_openssh_c_lp5_04.question.fex

Question 10: ✔ Correct

What is the full path and filename of the file you should edit to configure the SSH daemon on the server system?

/etc/ssh/sshd_config ✔

Explanation

The **/etc/ssh/sshd_config** file configures the SSH daemon on the server system. Be aware of the following frequently used options for configuring an SSH server:

- **AllowUsers** lists users allowed to use SSH. If an **AllowUsers** line is used in the file, all users except those listed are denied access by default.
- **DenyUsers** lists users not allowed to use SSH. If a DenyUsers line is used in the file, all users except those listed are granted access by default. A DenyUsers entry overrides an AllowUsers entry.
- **Protocol** specifies which protocols SSH allows when accessing the SSH server.
- **ListenAddress** gives the addresses that SSH should use when listening for requests. By default, the server listens on all IP addresses assigned to it. Use this line to specify specific addresses.
- **Port** specifies the port number. The default is 22. Use this line to change the default.
- **PasswordAuthentication** disables password authentication when set to *no*.
- **UsePAM** enables the Pluggable Authentication Modules (PAM) interface between sshd and the system.
- **PermitRootLogin** specifies whether users can log in as root over SSH.

References

15.6.6 OpenSSH Configuration Facts

q_openssh_c_lp5_05.question.fex