15.6.3 OpenSSH Facts

OpenSSH is a tool that encrypts network traffic over a network connection. OpenSSH is an open source implementation of the Secure Shell (SSH) protocol and implemented by default on most Linux distributions.

This lesson covers the following topics:

- Key facts
- Steps to establish an SSH connection

Key Facts

Be aware that SSH:

- Uses a public and private key pair to encrypt and transfer a symmetric key that is then used by both hosts to encrypt and decrypt transmissions during the SSH session. The public key is available to all users. The private key is kept secure and is never shared.
- Can use associated key management software and scripts to automate the exchange of public keys.
- Can be used to create a secure tunnel through which other unsecure network protocols, such as IMAP, POP3, SMTP, and X server traffic can be transmitted.
- Is available in two versions:
  - SSH version 1 (SSH1) is an older, less secure version of SSH. SSH1 only supports RSA encryption.
  - SSH version 2 (SSH2) is the current standard SSH implementation. It can use either DSA or RSA encryption.

Steps to Establish an SSH Connection

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

1. A client running SSH establishes a connection to any system running the SSH daemon (sshd) over port 22.
2. The computers determine which SSH version to use based on the specifications in the configuration files. Typically, this is SSH2.
3. The server sends one of the following public keys from the **/etc/ssh/** directory to the client:
   - **ssh_host_key.pub** (This is the SSH1 public key.)
   - **ssh_host_rsa_key.pub** (This is the SSH2 public key when using RSA. The associated private key file is **ssh_host_rsa_key**.)

- **ssh_host_dsa_key.pub** (This is the SSH2 public key when using DSA. The associated private key file is **ssh_host_dsa_key**.)

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. One of the following occurs:
    - If SSH1 is being used, the client generates a 256-bit symmetric key. It then uses the server's public key to encrypt the symmetric key and then sends it to the server. Because the secret key was encrypted with the public key, it can only be decrypted by the server using its private key.
    - If SSH2 is being used, the server and the client use the Diffie-Hellman key exchange system to agree on a symmetric key that will be used to encrypt data for the rest of the session. The secret key is not actually transmitted over the network.
6. The data transmitted between hosts is encrypted and decrypted using the same symmetric key.