15.6 OpenSSH

As you study this section, answer the following questions:

- What are the differences between symmetric and asymmetric encryption?
- When would you use the Diffie-Hellman Key Exchange encryption standard?
- Which encryption standards are supported by SSH1?
- Which encryption standards are supported by SSH2?
- Where does a client store public keys it has received from SSH servers?
- Which keys are sent to the client when establishing an SSH session?
- Which file should you edit to configure the SSH daemon on the server?
- Which file overrides the client's SSH configuration on a per-user basis?
- What **ssh** command would you use to log in to a server, execute a command, and return to the local system's shell prompt?

In this section, you will learn to:

- Configure OpenSSH.

Key terms for this section include the following:

Key Terms	Definition
Encryption	Encryption is a security technique that encodes information so that only someone with the proper key can decode it.
Symmetric key encryption	Symmetric key encryption (also known as secret key encryption, pre-shared key, or private key encryption) uses only one key to encrypt and decrypt data.
Asymmetric key encryption	Asymmetric key encryption (also known as public key encryption) uses two keys that are mathematically related. Both keys together form a key pair.
Public key	A public key is part of a key pair used in asymmetric encryption. It is is made available to anyone. Data encrypted with the public key can be decrypted using only the private key.
Private key	A private key is used in both symmetric and asymmetric encryptions. The private key is kept secret. In asymmetric encryption, data encrypted with the public key is decrypted with the private key. In symmetric encryption the private key both encrypts and decrypts.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Linux Pro	4.3 Monitor and manage system access • Manage remote connections

CompTIA Linux+	2.3 Given a scenario, create, modify, and redirect files. • File and directory operations ◦ scp 2.5 Summarize and explain server roles. • SSH 3.2 Given a scenario, configure and implement appropriate access and authentication methods. • SSH ◦ known-hosts ◦ config • PKI ◦ Private keys ◦ Public keys 3.6 Given a scenario, backup, restore, and compress files. • Off-site/off-system storage ◦ SFTP ◦ SCP