

Real-World Scenario 15-3: Making an SSH Connection

Scenario: A company you consult for wants to make secure connections to two Linux systems so that they can be remotely controlled in the command-line. The company does not want to use the deprecated Telnet utility. You decide to recommend the SSH protocol because of its known security advantages over Telnet.

What is SSH?

What port does it use, and which computers should have that port open?

What kind of secure algorithm does it support?

What program(s) can you use to remotely control the Linux systems from the command-line?

Real-World Scenario 15-3 Solution

SSH stands for Secure Shell, and it is a cryptographic protocol used to secure communications and command-line–based remote login. It uses port 22 by default. The computer that will be logged in to needs to have SSH installed and inbound port 22 open. SSH2 (as of the writing of this book) is the more secure version of SSH. It supports public key authentication using certificates (X.509), RSA, and DSA. File transfer can be secured by using SFTP. You can also secure the copying of files by using SCP. By default, these use TCP as the transport mechanism, but they can also use STCP. For these file transfers it supports the 3DES, AES, and Blowfish symmetric algorithms.

The most commonly used program to remotely control Linux systems in the command-line is the PuTTY program. It is an open source terminal emulator that allows control over the remote computer and network file transfer. It has support for a wide variety of operating systems. Other SSH clients include SuperPutty, Kitty, Xshell, Open SSH, Dropbear, and Tera Term, though their support for operating systems will vary.

Video Solution: Watch the video solution “15-3: Making an SSH Connection.”