SSH Overview

Password SSH login

Typically when you setup a SSH remote server, you would login by entering the remote user's username and its password that you are logging as. The SSH server program will ask OS "I got this username and its password" Can I let him in and be connected, if the credentials are correct, then SSH allows you to be authenticated and be on your way.

Public-key authentication

The other way that the SSH server can authenticate you is via public-key authentication. Specific algorithm can vary but usually is RSA/DSA.

The way it works is that the user who is trying to log into the server will be creating two keys, one public key, and one private key using `ssh-keygen` program.

You can then place the public key into the remote server's `~/.ssh/authorized_keys` file, then when you attempt to connect to SSH with a username + your private key file using the `-i` option, SSH will ask the OS "i got this username and a private key" can he be let in? If yes then SSH will look at your private key to verify that it matches the public key in `authorized_keys` file then you are allowed in.

Specific process of SSH authentication

A secure communication channel has to be first established before authentication. The secure communication is established using symmetric key encryption. This is because asymmetric key pairs are only used for authentication and not encrypting entire connection.

After the secure communication between server and client is established the client must be authenticated to be allowed access. The server will use the client's public key to issue a challenge message to the client, if the client can prove that it is able to decrypt the message, which mean that it has the associated private key. Then server can allow the client in.

known_hosts file

The `known_hosts` file is used to authenticate the servers, just like how `authorized_keys` is used to authenticate users. This file contain the server's public key, and every time you connect to an SSH server, it will show you their public key along with a proof that it has the corresponding private key.

Revision #2
Created 2023-02-08 23:19:15 UTC by Tamarine
Updated 2023-02-09 00:30:36 UTC by Tamarine