



SSH教程

——by Wangdoc

目录

1. SSH 基本知识

SSH 基本知识

SSH (Secure Shell 的缩写) 是一种网络协议，用于加密两台计算机之间的通信，并且支持各种身份验证机制。

实务中，它主要用于保证远程登录和远程通信的安全，任何网络服务都可以用这个协议来加密。

目录 [隐藏]

1. [SSH 是什么](#)
2. [历史](#)
3. [SSH 架构](#)

1. SSH 是什么

历史上，网络主机之间的通信是不加密的，属于明文通信。这使得通信很不安全，一个典型的例子就是服务器登录。登录远程服务器的时候，需要将用户输入的密码传给服务器，如果这个过程是明文通信，就意味着传递过程中，线路经过的中间计算机都能看到密码，这是很可怕的。

SSH 就是为了解决这个问题而诞生的，它能够加密计算机之间的通信，保证不被窃听或篡改。它还能对操作者进行认证 (authentication) 和授权 (authorization)。明文的网络协议可以套用在它里面，从而实现加密。

2. 历史

1995年，芬兰赫尔辛基工业大学的研究员 Tatu Ylönen 设计了 SSH 协议的第一个版本（现称为 SSH 1），同时写出了第一个实现（称为 SSH1）。

当时，他所在的大学网络一直发生密码嗅探攻击，他不得不为服务器设计一个更安全的登录方式。写完以后，他就把这个工具公开了，允许其他人免费使用。

SSH 可以替换 rlogin、TELNET、FTP 和 rsh 这些不安全的协议，所以大受欢迎，用户快速增长，1995年底已经发展到五十个国家的20,000个用户。SSH 1 协议也变成 IETF 的标准文档。

1995年12月，由于客服需求越来越大，Tatu Ylönen 就成立了一家公司 SCS，专门销售和开发 SSH。这个软件的后续版本，逐渐从免费软件变成了专有的商业软件。

SSH 1 协议存在一些安全漏洞，所以1996年又提出了 SSH 2 协议（或者称为 SSH 2.0）。这个协议与1.0版不兼容，在1997年进行了标准化，1998年推出了软件实现 SSH2。但是，官方的 SSH2 软件是一个专有软件，不能免费使用，而且 SSH1 的有些功能也没有提供。

1999年，OpenBSD 的开发人员决定写一个 SSH 2 协议的开源实现，这就是 OpenSSH 项目。该项目最初是基于 SSH 1.2.12 版本，那是当时 SSH1 最后一个开源版本。但是，OpenSSH 很快就完全摆脱了原始的官方代码，在许多开发者的参与下，按照自己的路线发展。OpenSSH 随 OpenBSD 2.6 版本一起提供，以后又移植到其他操作系统，成为最流行的 SSH 实现。目前，Linux 的所有发行版几乎都自带 OpenSSH。

现在，SSH-2 有多种实现，既有免费的，也有收费的。本书的内容主要是针对 OpenSSH。

3. SSH 架构

SSH 的软件架构是服务器-客户端模式（Server - Client）。在这个架构中，SSH 软件分成两个部分：向服务器发出请求的部分，称为客户端（client），OpenSSH 的实现为 ssh；接收客户端发出的请求的部分，称为服务器（server），OpenSSH 的实现为 sshd。

本教程约定，大写的 SSH 表示协议，小写的 ssh 表示客户端软件。

另外，OpenSSH 还提供一些辅助工具软件（比如 ssh-keygen、ssh-agent）和专门的客户端工具（比如 scp 和 sftp），这个教程也会予以介绍。