安全登录守护进程

内容提要

1. 熟悉 OpenSSH 的功能
2. 熟悉 OpenSSH 的相关文件
3. 理解 OpenSSH 的密钥认证
4. 熟悉 OpenSSH 客户命令的使用
5. 掌握密钥对的生成和分发

OpenSSH 和密钥认证协议

OpenSSH 简介

管理员时常需要同时管理通过网络相连的分散于各处的多台主机，而类 UNIX 操作系统最大的特色就是可以进行远程登录并进行管理。UNIX 系统很早就有（r 族命令：rlogin、rsh、rcp）用于实现远程登录、远程命令执行、远程文件传输的功能。但遗憾的是他们都不安全。

SSH（Secure SHell）协议是 C/S 模式协议，即区分客户端和服务器端。一次成功的 ssh 会话需要两端通力合作来完成。 所有使用 SSH 协议的通讯，包括口令，都会被加密传输。传统的 telnet 和 ftp 之所以不安全，就是因为他们使用纯文本口令，并被明文发送。这些信息可能会被截取，口令可能会被检索，然后未经授权的人员可能会使用截取的口令登录进你的系统而对你的系统造成危害。

与使用传统 r 族命令和 telnet 命令最大的不同之处就是 SSH 还添加了密钥认证机制。主机密钥用于识别主机的身份（安装后自动生成，一般无需变更）；用户个人的密钥用于识别用户身份（需要用户自己生成）。

OpenSSH [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5vcGVuc3NoLmNvbQ%3D%3D] 是 SSH 协议的免费开源实现。它用安全、加密的网络连接工具（s 族命令：ssh、scp、sftp）代替了 telnet、 rlogin、rsh、rcp 和 ftp 等工具。你应该尽可能地使用 OpenSSH 的工具集合来避免这些安全问题。OpenSSH 支持 SSH 协议的版本 1.3、1.5、和 2。自从 OpenSSH 的版本 2.9 以来，默认的协议是版本 2，该协议支持 RSA 和 DSA，默认使用 RSA 密钥。OpenSSH 既支持基于 PAM 的用户口令认证同时也支持用户密钥认证。

密钥认证协议

OpenSSH 使用非对称密钥的 RSA 和 DSA 认证协议来认证用户。RSA 和 DSA 认证承诺不必提供密码就能够同远程系统建立连接，这是 SSH 的主要魅力之一。

RSA/DSA 密钥认证协议的基本工作原理：

1. 密钥由一对组成：一把专用密钥（亦称私钥）和一把公用密钥（亦称公钥）。
2. 密钥对由客户端生成，私钥由用户自己保管，并将公钥散播到需要认证之处（登录服务器端）。
3. 公钥用于对消息进行加密，只有拥有私钥的人才能对该消息进行解密。
4. 公钥只能用于加密，而私钥只能用于对由匹配的公钥编码的消息进行解密。

使用RSA/DSA 密钥认证协议的 ssh 登录过程：

1. 本地主机使用 ssh 客户命令告诉远程主机的 sshd 守护进程想使用 RSA/DSA 认证协议登录。
2. 远程主机的 sshd 守护进程会生成一个随机数，并使用存储于该机上的公钥对这个随机数进行加密。
3. 远程主机的 sshd 守护进程把加密了的随机数发回给正在本地主机上运行的 ssh 客户。
4. 本地主机的 ssh 客户用密钥对中的私钥对这个随机数进行解密后，再把它发回给远程主机的 sshd 守护进程。
5. 远程主机的 sshd 守护进程进行判断，若密钥对匹配，则允许登录。

OpenSSH 及其相关文件

CentOS 默认安装了 openssh 的客户端和服务器端软件包，您也可以使用 yum 来安装：

```
# yum install openssh-client openssh-server
```

OpenSSH服务器配置文件、客户端系统配置文件和客户端用户配置文件的位置和文件名称：

- OpenSSH服务器配置文件 — /etc/ssh/sshd_config
- OpenSSH客户端系统配置文件 — /etc/ssh/ssh_config
- OpenSSH客户端用户配置文件 — $HOME/.ssh/config

客户命令会依次读取如下条目（优先级由高到低）决定其行为：

- 命令行参数选项
- 用户自家目录 $HOME/.ssh/config 配置文件
- 系统客户配置文件 /etc/ssh/ssh_config

密钥相关文件：

- 主机密钥相关
  - /etc/ssh/ssh_host_key：主机 RSA 认证私钥(SSH-1)
  - /etc/ssh/ssh_host_key.pub：主机 RSA 认证公钥(SSH-1)
  - /etc/ssh/ssh_host_dsa_key：主机 DSA 认证私钥(SSH-2)
  - /etc/ssh/ssh_host_dsa_key.pub：主机 DSA 认证公钥(SSH-2)
  - /etc/ssh/ssh_host_rsa_key：主机 RSA 认证私钥(SSH-2)

- /etc/ssh/ssh_host_rsa_key.pub：主机 RSA 认证公钥(SSH-2)
- /etc/ssh/ssh_known_hosts：已知的主机密钥的系统级列表

- 用户密钥相关
  - ~/.ssh/identity：用户默认的 RSA1 身份认证私钥(SSH-1)。
  - ~/.ssh/identity.pub：用户默认的 RSA1 身份认证公钥(SSH-1)。
  - ~/.ssh/id_dsa：用户默认的 DSA 身份认证私钥(SSH-2)。
  - ~/.ssh/id_dsa.pub：用户默认的 DSA 身份认证公钥(SSH-2)。
  - ~/.ssh/id_rsa：用户默认的 RSA 身份认证私钥(SSH-2)。
  - ~/.ssh/id_rsa.pub：用户默认的 RSA 身份认证公钥(SSH-2)。
  - ~/.ssh/authorized_keys：用于存放所有已知用户的公钥。

配置 OpenSSH 服务器

在安装了openssh-server 软件包之后，默认的配置即可运行良好。

您可以使用 service 命令启动、停止或重启 sshd 守护进程。

```
# service sshd start
# service sshd stop
# service sshd restart
```

OpenSSH 服务器的配置文件是 /etc/ssh/sshd_config。配置文件中的语句说明参见：http://lamp.linux.gov.cn/OpenSSH/sshd_config.html [http://www.proxyserve.net/index.php?q=aHR0cDovL2xhbXAubGludXguZ292LmNuL09wZW5TU0gvc3NoZF9jb25maWcuaHRtbA%3D%3D]

使用 OpenSSH 客户端

OpenSSH 客户端包括 ssh、scp、sftp 命令。有关这些命令的基本使用参见 基本网络操作命令。

下面重点说说用户密钥认证客户配置过程。

密钥对的生成和分发

1、在服务器方创建目录和文件（若不存在）

```
[smart@centos5 ~]$ mkdir ~/.ssh
[smart@centos5 ~]$ chmod 700 ~/.ssh
[smart@centos5 ~]$ touch ~/.ssh/authorized_keys
[smart@centos5 ~]$ chmod 600 ~/.ssh/authorized_keys
```

2、在客户端生成密钥对

```
[smart@backup ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/smart/.ssh/id_dsa):
Created directory '/home/smart/.ssh'.
Enter passphrase (empty for no passphrase):        # 输入私钥保护短语
Enter same passphrase again:
Your identification has been saved in /home/smart/.ssh/id_dsa.
Your public key has been saved in /home/smart/.ssh/id_dsa.pub.
The key fingerprint is:
2a:ff:fc:1e:6a:07:90:8d:dd:51:16:e3:70:57:33:28 smart@backup
[smart@backup ~]$ ll .ssh
total 8
-rw------- 1 smart smart 668 Mar 14 20:19 id_dsa
-rw-r--r-- 1 smart smart 602 Mar 14 20:19 id_dsa.pub
```

3、将客户端生成的公钥分发到服务器端

```
[smart@backup ~]$ cat .ssh/id_dsa.pub | ssh 192.168.0.55 "cat - >> ~/.ssh/authorized_keys"
The authenticity of host '192.168.0.55 (192.168.0.55)' can't be established.
RSA key fingerprint is 3c:45:c5:7d:10:02:10:34:d6:d6:b4:9b:89:15:7d:e6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.55' (RSA) to the list of known hosts.
smart@192.168.0.55's password:        # 输入 smart 用户在 192.168.0.55 上的用户口令
[smart@backup ~]$
```

4、以密钥认证方式进行远程登录

```
[smart@backup ~]$ ssh 192.168.0.55
Enter passphrase for key '/home/smart/.ssh/id_dsa':        # 输入私钥保护短语
[smart@centos5 ~]$
```

若您在使用 ssh-keygen 命令生成密钥对时没有设置私钥保护短语（即直接回车），则使用 ssh 登录时将直接进入远程系统。这在 **cron** 任务中包含有 **s** 族命令、**rsync** 等命令时很有用。

参考

- http://www.snailbook.com/ [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5zbmFpbGJvb2suY29tLw%3D%3D]
- http://www.howtoforge.com/ssh-best-practices [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy5ob3d0b2ZvcmdlLmNvbS9zc2gtYmVzdC1wcmFjdGljZXM%3D]
- http://www-900.ibm.com/developerWorks/cn/linux/security/openssh/part1/index.shtml [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy05MDAuaWJtLmNvbS9kZXZlbG9wZXJXb3Jrcy9jbi9saW51eC9zZWN1cml0eS9vcGVuc3NoL3BhcnQxL2luZGV4LnNodG1s]
- http://www-900.ibm.com/developerWorks/cn/linux/security/openssh/part2/index.shtml [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy05MDAuaWJtLmNvbS9kZXZlbG9wZXJXb3Jrcy9jbi9saW51eC9zZWN1cml0eS9vcGVuc3NoL3BhcnQyL2luZGV4LnNodG1s]

- http://www-900.ibm.com/developerWorks/cn/linux/security/openssh/part3/index.shtml [http://www.proxyserve.net/index.php?q=aHR0cDovL3d3dy05MDAuaWJtLmNvbS9kZXZlbG9wZXJXb3Jrcy9jbi9saW51eC9zZWN1cml0eS9vcGVuc3NoL3BhcnQzL2luZGV4LnNodG1s]
- 显示源文件
- 登录