设置 Linux 服务器使用密钥认证 SSH 服务

1. 简介

暴力破解攻击是以枚举方式对弱口令进行猜测的攻击手段。暴露于网络的应用经常会受到这种攻击尝试。Linux 服务器的 SSH 端口是常见的暴力破解攻击的目标。对服务器来说，攻击成功等同于服务器管理权失陷，危害极大。

通常，我们通过周期性更改密码和增加密码复杂度抵御此类攻击，但是过于频繁更改密码或者过于复杂的密码会造成密码本身难于使用，而过低的更换周期或者过于简单的密码则无法起到防护作用。实际操作中，基于密码的认证很难在便捷性与安全性中找到平衡点。

SSH 协议支持使用密钥方式认证，正确的使用完全可以替代密码登录，达到既便捷又安全的目标。SSH 的密钥认证是基于非对称加密算法的认证方式，其使用数字签名校验替代密码比对实现用户认证，算法安全性由非对称加密算法本身决定，密钥一般随机生成长度远大于人工可以记忆或有限时间能够枚举的数据长度，从理论上难于被暴力破解。

本文我们介绍如何在 Linux 服务器上开启 SSH 服务的密钥认证，同时关闭远程密码登录。

2. 客户端生成 SSH 密钥对

使用密钥认证登录SSH服务，首先要在客户端电脑上生成SSH密钥对。在Linux、MacOS、BSD、Windows 10/11主机上，我们使用OpenSSH中的ssh-keygen工具完成这件工作。在命令行窗口中，直接运行ssh-keygen命令：

```
$ ssh-keygen
```

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/username/.ssh/id_rsa):
Created directory '/home/username/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/username/.ssh/id_rsa
Your public key has been saved in /home/username/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:vHB9DQ0TwQXWH+9Uag18PgQkup9LDKxW0v4O20TsJaA username@localhost.localdomain
```

默认情况下，ssh-keygen将为用户生成RSA算法的密钥对，长度为3072位。生成密钥时，会提示用户提供密码对私钥加密，不同于用户口令，这个密码仅在本地使用，用于防止私钥泄漏。当然，如果对自己电脑安全完全有信心，私钥也可以不加密存放(**不建议**)。工具ssh-keygen一般不需要添加参数运行，根据Linux系统安全理念，成熟的发行版本应实现默认即安全，即用默认参数运行时就能获得安全的结果。

需要注意的是，生成的密钥对中，~/.ssh/id_rsa.pub是公钥，无需保密；**~/.ssh/id_rsa是私钥，要时刻保密，不能与他人分享。如果有多台电脑需要访问服务器，应该在每台电脑上使用上述过程生成自己的独立密钥对，**而不是将私钥复制到每台电脑上。

在Windows 10和Windows 11系统中，也已经预装了OpenSSH客

户端，进入 Powershell 或者 CMD 窗口就可以使用 ssh 系列命令，用法与上述过程相同。常见第三方工具一般也支持使用 OpenSSH 格式的密钥，但是 PUTTY（一种 Windows 下常用的 SSH 第三方工具）例外。不过 PUTTY 自带了 puttygen.exe 工具用于生成密钥对，或者转换 OpenSSH 的密钥对使用。其具体方法我们将在后续文章里说明，用户也可以自行在互联网上查找。

3. 上传公钥到服务器

OpenSSH 服务器在默认情况下已经支持密钥登陆，只要我们将生成的公钥内容添加到服务器指定位置，即可开始使用密钥认证方式。

上传公钥到服务器有两种方法，一种是使用 ssh-copy-id 命令自动完成（推荐），也可以手动添加。使用 ssh-copy-id 时，命令行参数与使用 ssh 命令登陆服务器完全相同，直接运行：

```
$ ssh-copy-id username@server_address
```

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/username/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

username@server_address's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'username@server_address'"
and check to make sure that only the key(s) you wanted were added.
```

命令提示用户输入当前 SSH 登陆口令，认证通过后，ssh-copy-id 命令会将本地存在的，但是服务器上没有保存的公钥全部上传到

目标位置，上传完成后命令提示上传成功的密钥数量并自动退出。

我们也可以手动添加 SSH 公钥到服务器，运行命令：

```
cat ~/.ssh/id_rsa.pub | ssh username@server_address "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod -R go-rwx ~/.ssh"
```

```
username@server_address's password:
```

命令执行成功时，除了服务器用户认证时输入密码的提示，不会有其它提示。

在服务器上,授权的用户公钥保存于~/.ssh/authorized_keys 文件中，上述命令做了三件事 ，一是如果~/.ssh 目录不存在，则创建它；二是将公钥保存在~/.ssh/authorized_keys 文件中；三是修正存放密钥的目录的权限，确保用户以外无人可以访问其中内容。这也是 ssh-copy-id 实际完成的工作。

4. 使用密钥认证登陆服务器

密钥添加完成后立即生效，使用命令登陆服务器(登陆命令和以前相比无变化)：

```
$ ssh username@server_address
```

如果私钥没有加密存放,则系统不提示输入密码,登陆直接完成。如果私钥设置了密码，此时按照系统提示输入私钥的加密密码，即可登陆成功。

5. 关闭密码登录

密钥登陆设置成功后，我们建议关闭密码登陆方式，防止外部暴力破解攻击。关闭密码登陆可以通过编辑 SSH 服务端配置文件完成。使用常用编辑器打开/etc/ssh/sshd_config 文件(需要管理员 root 权限)，例如，用 vi 编辑器：

```
# vi /etc/ssh/sshd_config
```

找到如下内容：

```
#PasswordAuthentication yes
```

或者(行首没有“#”字符)：

```
PasswordAuthentication yes
```

改为：

```
PasswordAuthentication no
```

请注意，行首有“#”字符的，表明本行配置未生效（被注释状态），一定要删除行首的“#”字符。保存修改，让 SSH 服务端进程重新加载，使用命令：

```
# systemctl reload sshd
```

或者以下命令(CentOS 6 或者更老的没有使用 systemd 系统的发行版，需要 SysV 方式管理服务)：

```
# service sshd reload
```

完成上述配置后，建议找一台没有密钥授权的客户端电脑，尝试 SSH 连接,验证密码登陆确实已经成功禁止,确保安全措施落实到位。

6. 总结

本文我们介绍了使用密钥登陆 SSH 服务的方法，包含客户端电脑配置 SSH 密钥对，服务器安装 SSH 密钥对以及禁止密码登陆的设置方法。使用本文介绍的方法，用户可以完全关闭 SSH 服务的密码认证方式，彻底杜绝外部针对 SSH 用户密码的暴力破解攻击。我们强烈推荐校园网 Linux 用户在自己负责的服务器和工作站上落实本文介绍的方法，提升服务器抵御外部攻击的能力。