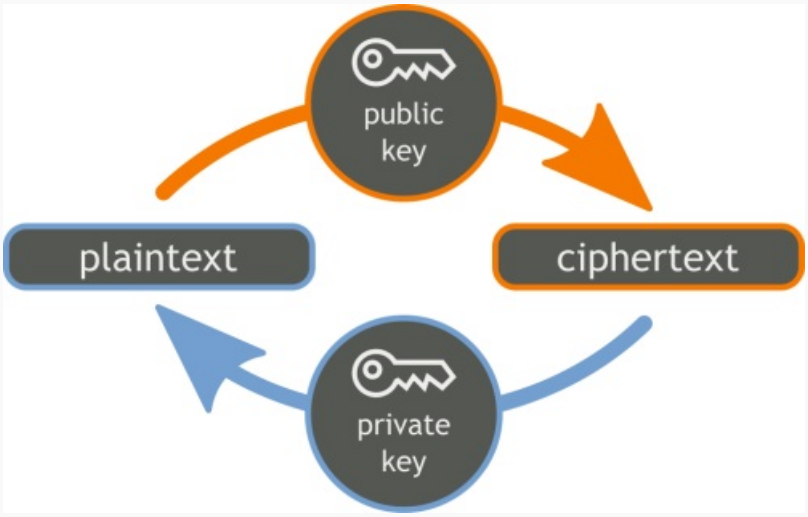
SSH 使用密钥登录并禁止口令登录实践

2015-7-8 14:04　收藏: *10*

参考原文：http://wsgzao.github.io/post/ssh/作者： wsgzao
文章地址：https://linux.cn/article-5776-1.html



前言

无论是个人的VPS还是企业允许公网访问的服务器，如果开放22端口的SSH密码登录验证方式，被众多黑客暴力猜解捅破菊花也可能是经常发生的惨 剧。企业可以通过防火墙来做限制，普通用户也可能借助修改22端口和强化弱口令等方式防护，但目前相对安全和简单的方案则是让SSH使用密钥登录并禁止口 令登录。

> 这是最相对安全的登录管理方式

生成PublicKey

> 建议设置并牢记passphrase密码短语，以Linux生成为例

Linux：ssh-keygen -t rsa

[私钥 (id_rsa) 与公钥 (id_rsa.pub)]

Windows：SecurCRT/Xshell/PuTTY

[SSH-2 RSA 2048]

```
#生成SSH密钥对
ssh-keygen -t rsa

Generating public/private rsa key pair.
#建议直接回车使用默认路径
Enter file in which to save the key (/root/.ssh/id_rsa):
#输入密码短语（留空则直接回车）
Enter passphrase (empty for no passphrase):
#重复密码短语
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
aa:8b:61:13:38:ad:b5:49:ca:51:45:b9:77:e1:97:e1 root@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|    .o.          |
|    ..   . .     |
|   .  . . o o    |
| o.  . . o E     |
|o.=   . S .      |
|.*.+   .         |
|o.*   .          |
```

```
| . + .           |
|  . o.           |
+-----------------+
```

复制密钥对

也可以手动在客户端建立目录和authorized_keys，注意修改权限

```
#复制公钥到无密码登录的服务器上,22端口改变可以使用下面的命令
#ssh-copy-id -i ~/.ssh/id_rsa.pub "-p 10022 user@server"
ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.15.241

```

修改SSH配置文件

```
#编辑sshd_config文件
vi /etc/ssh/sshd_config

#禁用密码验证
PasswordAuthentication no
#启用密钥验证
RSAAuthentication yes
PubkeyAuthentication yes
#指定公钥数据库文件
AuthorsizedKeysFile .ssh/authorized_keys

```

重启SSH服务前建议多保留一个会话以防不测

```
#RHEL/CentOS系统
service sshd restart
#ubuntu系统
service ssh restart
#debian系统
/etc/init.d/ssh restart
```

手动增加管理用户

可以在== 后加入用户注释标识方便管理

```
echo 'ssh-rsa XXXX' >>/root/.ssh/authorized_keys

# 复查
cat /root/.ssh/authorized_keys
```

扩展阅读

- SSH原理与运用 - http://www.ruanyifeng.com/blog/2011/12/ssh_remote_login.html
- 使用公钥验证登录 SSH - https://www.linode.com/docs/networking/ssh/use-public-key-authentication-with-ssh