

实验名称：使用私钥访问 SSH 服务器

实验原理：非对称加密算法生成一对密钥（公钥和私钥），其中，私钥由一方安全保管，而公钥则可对外公开，如果用其中一个密钥加密数据，只有对应密钥才可以解密，利用这一特性可以实现远程服务器对用户身份的认证。在使用私钥访问 SSH 服务器时，用户可以提前将公钥上传至服务器，当用户发起登陆请求时，用户方将利用私钥对服务器发来的随机字符串进行加密，并将密文发送回服务器；服务器收到密文后会根据用户方提供的公钥对密文进行解密，如果成功则用户身份得到验证。

实验环境：一台 Ubuntu23.04 虚拟机、一台 Windows11 本地计算机

实验步骤：

1. 配置实验环境

- 1) 本实验使用一台基于 VMware Workstation Pro 搭载 Ubuntu23.04 的虚拟机 Server 和一台本地搭载 Windows11 的计算机进行演示。系统信息如下图所示。

操作系统名称	Ubuntu 23.04	版本	Windows 11 专业版 Insider Preview
操作系统类型	64 位	版本	22H2
GNOME 版本	不可用	安装日期	2023/5/8
窗口系统	Wayland	操作系统版本	23451.1000
虚拟化	VMware	体验	Windows Feature Experience Pack 1000.23451.1000.0
内核版本	Linux 6.2.0-20-generic		

2. 配置 Server

- 1) 虚拟机 Server 在本实验中模拟服务器。在终端中输入命令 `sudo apt-get install openssh-server -y` 安装 openssh 服务，安装完成后再输入命令 `sudo service ssh restart` 开启 SSH 服务，再输入命令 `service ssh status`，显示如下图所示说明开启成功。

```
root@server:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Drop-In: /etc/systemd/system/ssh.service.d
            └─00-socket.conf
   Active: active (running) since Mon 2023-05-08 19:12:59 CST; 9min ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 4493 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4494 (sshd)
   Tasks: 1 (limit: 4579)
   Memory: 3.6M
   CPU: 50ms
   CGroup: /system.slice/ssh.service
           └─4494 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

3. 使用密码连接 Server

- 1) 在本地计算机使用管理员身份运行 PowerShell，输入命令 `Add-WindowsCapability -Online -Name OpenSSH.Client`，安装 SSH 服务，安装成功如下图所示。

```
PS C:\WINDOWS\system32> Add-WindowsCapability -Online -Name OpenSSH.Client

Path          :
Online        : True
RestartNeeded : False
```

- 2) 首先尝试使用密码连接。在本地计算机使用管理员身份运行 PowerShell，输入命令 `ssh server@192.168.48.131`，输入 server 用户的登录密码，连接成功。

```

PS C:\WINDOWS\system32> ssh server@192.168.48.131
The authenticity of host '192.168.48.131 (192.168.48.131)' can't be established.
ED25519 key fingerprint is SHA256:9FCMeQubgfXKswkKCjSCpU1gNAjQg7WuuXexRNoPLbY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.48.131' (ED25519) to the list of known hosts.
server@192.168.48.131's password:
Welcome to Ubuntu 23.04 (GNU/Linux 6.2.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

4 更新可以立即应用。
要查看这些附加更新，请运行：apt list --upgradable

Last login: Tue May 9 16:47:50 2023 from 192.168.48.129
server@server: $

```

4. 使用密钥连接 Server

- 1) 在本地计算机以管理员身份运行 PowerShell，输入命令 `ssh-keygen -t ed25519`，有提示按回车即可。可以看到 `C:\Users\18313\.ssh\` 目录下新增了私钥文件 `id_ed25519` 和公钥文件 `id_ed25519.pub`。
- 2) 使用密码连接 Server，将公钥 `id_ed25519.pub` 复制到 `~/.ssh/authorized_keys` 文件。
- 3) 在 Server 终端输入命令 `sudo nano /etc/ssh/sshd_config`，将 `PasswordAuthentication` 更改为 `no`，关闭使用密码连接功能；将 `PubkeyAuthentication` 更改为 `yes`，启用使用密钥连接功能；将 `AuthorizedKeysFile` 设置为 `.ssh/authorized_keys`，指定公钥数据库文件；将 `PermitRootLogin` 改为 `yes`，启用以 `root` 身份登录功能。
- 4) 在 Server 终端输入命令 `service ssh restart`，重启 SSH 服务。
- 5) 在本地计算机以管理员身份运行 PowerShell，输入命令 `ssh -i .\id_ed25519 root@192.168.48.131`，使用私钥以 `root` 身份连接 `server`。连接成功如下图所示。

```

PS C:\WINDOWS\system32> ssh -i .\id_ed25519 root@192.168.48.131
Warning: Identity file .\id_ed25519 not accessible: No such file or directory.
Welcome to Ubuntu 23.04 (GNU/Linux 6.2.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

4 更新可以立即应用。
要查看这些附加更新，请运行：apt list --upgradable

Last login: Tue May 9 19:03:12 2023 from 192.168.48.129
root@server: #

```

- 6) 在本地计算机以管理员身份运行 PowerShell，输入命令 `ssh -p 999 root@192.168.48.131`，使用密码以 `server` 身份连接 `server`，其中 `999` 是 `server` 的登录密码。连接失败，如下图所示，说明成功关闭 SSH 使用密码登录功能。

```

PS C:\WINDOWS\system32> ssh -p 999 server@192.168.48.131
ssh: connect to host 192.168.48.131 port 999: Connection refused

```