日照职业技术学院

《Linux 企业运维实战》实训报告书

所学专业：

学　　号：

姓　　名：

指导教师：

项目 3　实训报告

实训时间：		实训人：	
实训名称 **3-5 配置远程控制任务**			
1.实训目标： ①分别配置服务器和客户机虚拟机的主机名和 IP 地址，网络均设置为桥接模式。 ②掌握创建公钥私钥的命令 ③掌握 SSH 服务主配置文件的修改与设置。 ④掌握重启 SSH 服务，并设置开机自动加载。 ⑤掌握 SSH 远程登录命令 ⑥掌握远程传输命令 scp 的使用 2.实训任务： ①实现基于口令的验证—用账户和密码来验证登录。 ②在配置的 sshd 服务中，设置禁止以 root 管理员的身份远程登录到服务器。 ③实现配置基于密钥验证方式，并进行远程登录验证 ④实现使用远程传输命令 scp，并进行远程登录验证。			
实训环境描述：GNOME 桌面环境			
实训操作过程及配置说明： **要求：需要写实训步骤，重要步骤请辅助截图**			

子任务 1：配置基于口令的验证 sshd 服务，并使用账户和密码来进行远程登录验证。

1、分别利用修改主机名的命令和网络配置的方法，设置两台虚拟机的主机名和 IP 地址，一台做服务器，一台做客户机，需特别注意两台虚拟机的网络配置方式一定要一致，此案例两台网络均设置为桥接模式。

服务器主机名修改为 server7-1，ip 地址配置为 192.168.10.1/24，网关 192.168.10.254

客户机主机名修改为 client7-1，ip 地址配置为 192.168.10.20/24，网关 192.168.10.254

2.本案例中防火墙默认策略允许 SSH 服务，不需要配置，使用命令查看防火墙默认是否放行 SSH 服务？

3. **在客户端，使用账户和密码进行远程登录口令验证。**

子任务 2：在以上配置的 sshd 服务中，禁止以 root 管理员的身份远程登录到服务器，并进行远程登录验证。禁止以 root 管理员的身份远程登录，可以大大降低被黑客暴力破解密码的概率。

（1）server7-1 服务器上，修改 sshd 服务的主配置文件 /etc/ssh/sshd_config 的 36 行的参数，实现不再允许 root 管理员远程登录。

（2）重启 sshd 服务程序，并设置 sshd 服务开机即启动

（3）在 client7-2 客户机上测试， root 管理员还能正常访问 sshd 服务吗，普通用户可以吗？

子任务 3：配置基于密钥验证方式，并进行远程登录验证。

（1）在服务器虚拟机 server7-1，创建新用户 student，并设置密码。

（2）在客户端主机 client7-2 中生成“密钥对”并进入.ssh 目录，分别查看公钥 id_rsa.pub 和私钥 id_rsa 信息，

（3）把客户端主机 client7-2 中生成的公钥文件传送至远程主机的 student 用户。

（4）在服务器 server7-1 中，修改 SSH 服务的主配置文件/etc/ssh/sshd_config，65 行参数，只允许密钥验证，拒绝传统的口令验证方式。

（5）在客户端 client7-2 上尝试使用 student 用户远程登录到服务器，此时无须输入密码也可成功登录，可登录字符命令 。并使用 SSH 命令参数-X 和 gedit 命令
使用 firefox 命令访问服务器主机上之前搭建的 Apache 服务器。

（6）在服务器 server7-1 上查看 client7-2 客户机的公钥是否传送成功。

子任务 4:使用远程传输命令 scp,并进行远程登录验证。远程传输命令 scp(secure copy)是一个基于 SSH 协议在网络之间进行安全传输的命令，其格式为“scp［参数］本地文件 远程帐户@远程 IP 地址:远程目录”。

（1）在服务器 server7-1 上 root 目录下创建文件 myweb.txt，并向远程客户主机 client7-2（192.168.10.20）上传输此文件。

（2)在客户主机 client7-2(192.168.10.20)上,进入 home 目录查看传输的 mytest.txt

文件已经接收到。
实训结果（可以是截屏图片）：
总结和分析：