

知识点1【nc命令的帮助信息】

知识点2【nc命令案例】

1、TCP端口扫描

2、创建TCP服务器

3、创建TCP客户端

4、创建UDP接收端

5、创建UDP发送端

知识点1【nc命令的帮助信息】

```
1 nc -h
```

- g<网关> 设置路由器跃程通信网关，最多可设置8个。
- G<指向器数目> 设置来源路由指向器，其数值为4的倍数。
- h 在线帮助。
- i<延迟秒数> 设置时间间隔，以便传送信息及扫描通信端口。
- l 使用监听模式，管控传入的资料。
- n 直接使用IP地址，而不通过域名服务器。
- o<输出文件> 指定文件名称，把往来传输的数据以16进制字码倾倒成该文件保存。
- p<通信端口> 设置本地主机使用的通信端口。
- r 乱数指定本地与远端主机的通信端口。
- s<来源位址> 设置本地主机送出数据包的IP地址。
- u 使用UDP传输协议。
- v 显示指令执行过程。
- w<超时秒数> 设置等待连线的时间。
- z 使用0输入/输出模式，只在扫描通信端口时使用。

知识点2【nc命令案例】

1、TCP端口扫描

```
1 nc -v -w 2 10.9.21.201 21-24
```

```
1 ubuntu12 +
edu@edu:~/work/tmp/net$ nc -v -w 2 10.9.21.201 21-24
nc: connect to 10.9.21.201 port 21 (tcp) failed: Connection refused
Connection to 10.9.21.201 22 port [tcp/ssh] succeeded!
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10
nc: connect to 10.9.21.201 port 23 (tcp) failed: Connection refused
nc: connect to 10.9.21.201 port 24 (tcp) failed: Connection refused
```

2、创建TCP服务器

```
1 nc -l 8000 #服务器端口为8000
```

3、创建TCP客户端

```
1 nc 10.9.21.211 9000 #其他TCP服务器的端口
```

4、创建UDP接收端

```
1 nc -lu 8000 #监听端口为8000
```

5、创建UDP发送端

```
1 nc -u 10.9.21.211 9000 #加入其他主机的UDP接收端口的9000
```