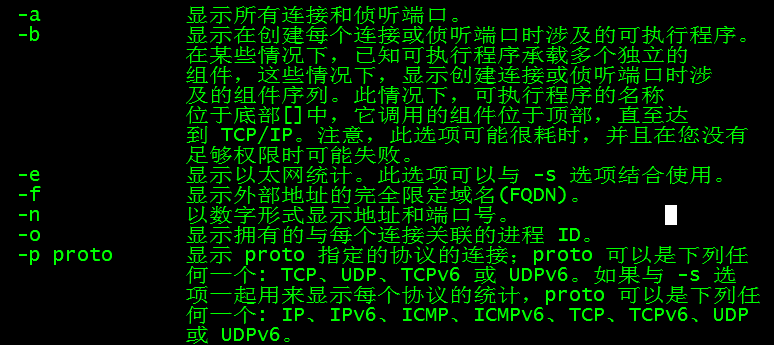
# 常用dos命令总结

|  |
| --- |
| gpedit.msc 组策略  nslookup ip地址查看器  explorer 打开计算机  lusrmgr 本地用户和组  services 打开服务  calc 打开计算器  devmgmt 设备管理器  regedit 注册表管理器  msconfig 配置系统启动服务  rsop 组策略集合  winver Windows版本信息  taskmgr 任务管理器  sfc /scannow 扫描错误并还原  mspaint 打开画图软件  magnify 打开放大镜  narrator 启用讲述人  eventvwr 事件查看器  logoff 注销 |

## 网络命令

### Netstat 查看端口

查看所有本机开放的端口；查看和外部建立的连接情况，参数如下图：



### Ipconfig 更新动态ip

Ipconfig /release 释放租用的动态地址

Ipconfig /renew 重新获取动态地址，相当于租用期重置

## Windows下使用nmap端口扫描

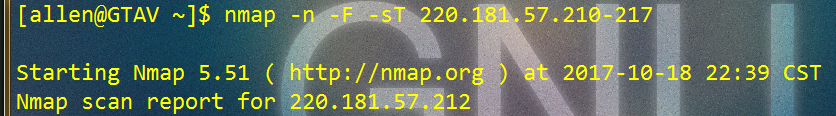
端口状态一般有以下几种：

|  |  |
| --- | --- |
| 状态 | 详细的参数说明 |
| Open | 端口是开启的，数据已经到达主机，并且在这个端口上有程序在接收数据 |
| Closed | 端口关闭，数据到达了主机，但是没有程序接收 |
| Filtered | 数据没有到达主机，返回空；表明数据被防火墙或者IDS过滤掉 |
| Unfiltered | 数据已经到达主机，没有被过滤掉，但是无法识别当前端口的状态 |
| Open|filtered | 端口没有返回值 |
| Closed|filtered | 发生在IP ID idle扫描中 |

### Nmap 常用参数

|  |  |
| --- | --- |
| -F | 扫描最常用的100个端口 |
| -v | 显示详细的扫描到的信息 |
| -n | 不进行域名解析，可以加快扫描速度 |
| -sT | 使用TCP扫描，默认选项；但最容易被防火墙拦截 |
| -PE | 使用ICMP协议进行扫描 |
| -sS | 使用SYN扫描，这是最隐秘的一种扫描方式 |
| -O | 扫描操作系统类型和版本 |
| -scanflags | 自定义扫描包 |
| -oN | 输出为普通文件 |
| -oX | 输出为XML文件 |
| -log-errors | 输出错误日志 |
| -packet-trace | 获取从当前主机到目标主机的所有节点 |
| -p port | 指定监听某个端口的状态 |
| -D ip1,ip2,ME | 同时使用多个诱饵IP进行扫描，把自己的ip藏在诱饵之中 |
| -S ip | 源地址欺骗：通过将自己的ip伪装成他人的ip进行扫描；让防火墙误认为是其他ip在使用； |
| -e |  |
| -T | 时间优化，通过优化时间来提高通过防火墙和IDS的 |
| -f | 将可疑的探测包进行分片（比如将tcp包拆分成多个ip包），某些简单的防火墙为了加快处理速度，可能不会进行重组检查，以此来避开检查 |
| -sl | 空闲扫描https://www.2cto.com/article/201505/396631.html |
| 全部参数 | https://www.2cto.com/article/201203/125686.html |

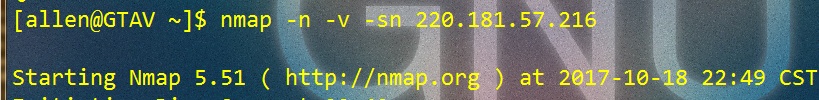
扫描网段内的所有机器，查看是否开启机器



扫描后的结果为：



只扫描机器，查看是否在线，不扫描端口



|  |  |
| --- | --- |
| TCP扫描 | |
| 概念 | 使用tcp的三次握手来进行扫描 |
| 特点 | 扫描速度快，准确性高，对操作者没有权限上的要求，但是容易被防火墙和IDS发现 |
| 原理 | Tcp三次握手   1. 客户端发送syn； 2. 服务器端返回syn+ack，表明端口开放 3. 客户端返回ack，表明建立连接 4. 客户端主动断开连接 |

示意图：

SYN

服务器

客户端

SYN+ACK

ACK

|  |  |
| --- | --- |
| SYN扫描 | |
| 概念 | 使用syn进行扫描 |
| 特点 | 这是最隐秘的一种扫描方式，因为客户端和服务器端连接的过程中，没有形成三次握手，所以不会被防火墙检测到或者留下日志记录，但是需要root权限；Windows下没有root的概念，这里指Linux |
| 原理 |  |

示意图

SYN

服务器

客户端

SYN+ACK

RST

|  |  |
| --- | --- |
| NULL扫描 | |
| 概念 | 这是一种反向扫描法，通过发送一个没有标志位的数据包给服务器，等待服务器的响应 |
| 特点 | 这种扫描方法更加隐蔽，但准确度也是最低的，这种方式只用来判断是否为Windows系统，因为Windows系统不遵循RFC793标准，不论端口是否开启，都返回RST包 |
| 原理 |  |

示意图

NULL(没有标志位)

服务器

客户端

RST

注意：不建议使用这种扫描，因为这种扫描准确率很低，而且很容易被过滤；如果要判断操作系统，只需要加上-O 参数即可

|  |  |
| --- | --- |
| Ack扫描 | |
| 概念 | 通过发送一个ack包给服务器，不论主机的端口是否开启，都会返回一个RST包，通过包中的ttl值判断端口是否开启 |
| 特点 |  |
| 原理 | Rst包中的ttl值如果大于64，表明端口关闭 |

示意图

ACK

服务器

客户端

RST(TTL<=64)

注意：也可以自定义扫描包，下图演示这种用法

