# 安全相关

## Linux系统扫描技术及安全防护

1. 主机扫描
   1. fping: 批量的扫描
      1. -g : 网段，
      2. -a （-u）：显示存活的主机（显示不存活的主机）
      3. -f：从文件读取要扫描的ip



* 1. hping：可以自定义tcp/ip包，不一定使用icmp（ubuntu下为hping3）
     1. -p：指定端口
     2. -S：发送syn包
     3. -a：伪造地址

（1）设置192.168.138.128 icmp不可用，即其他主机不能ping到：

128：

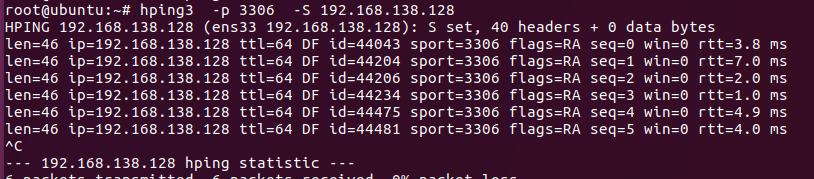


130：



不能够ping通128.

（2）hping加参数-S（注意是大写，小写表示源端口），使用tcp去ping128：

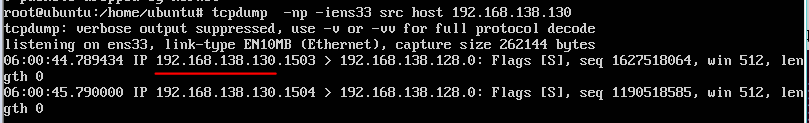


（3）hping加参数-a，伪造源ip，可用于Ddos攻击

在128上使用tcpdump -np -i网卡 src host 192.168.138.130

在130上发送hping -S 192.168.138.128

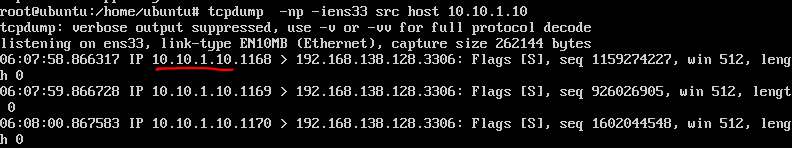
128截图：



在130上使用命令：hping -S 192.168.138.128 -a 10.10.1.10

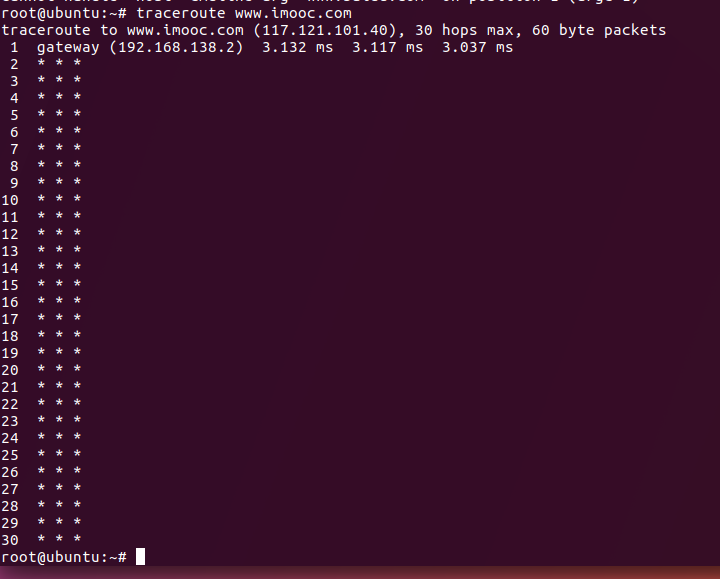


128:显示来自10.10.1.10的 ping：



1. 路由扫描
   1. traceroute
      1. 原理：发送udp包，设置udp端口>30000，设置TTL= 1，遇到路由器，TTL减一，等于0，回发ICMP包回到源主机，记录时间；设置TTL=2，遇到两个路由后，减为0，回发ICMP到源主机；。。。；直到目的主机，因为udp协议规定端口不能大于30000，所以返回端口不可达，源主机知道了到达目的主机的路由信息。
      2. 最多30跳

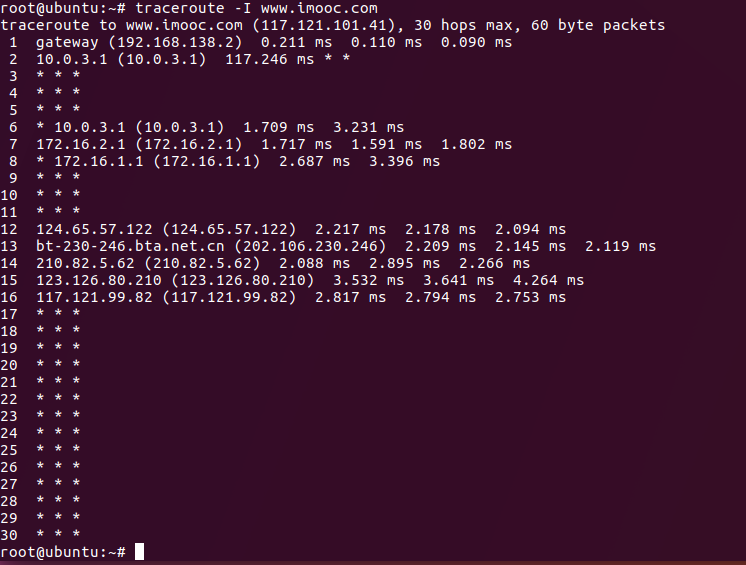
命令traceroute [www.imooc.com](http://www.imooc.com)



可以推测，imooc屏蔽了udp的扫描

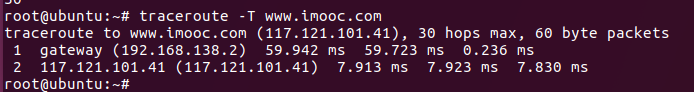
* + 1. 使用参数 -I使用ICMP协议扫描

traceeoute -I [www.imooc.com](http://www.imooc.com)

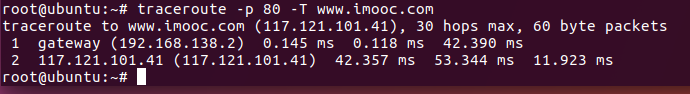


* + 1. 使用参数 -T 使用TCP协议扫描

traceroute -T [www.imooc.com](http://www.imooc.com)



加上端口参数 -p



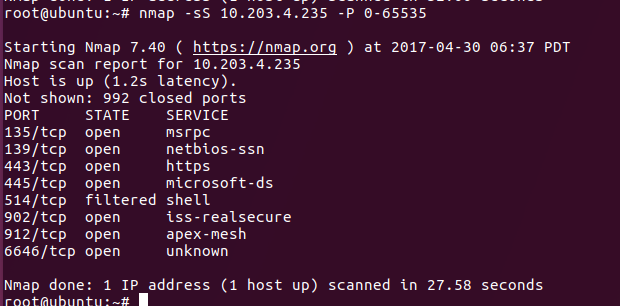
* 1. mtr

mtr [www.imooc.com](http://www.imooc.com)，可以动态显示丢包情况，在哪一个节点丢包



1. 批量服务扫描
   1. nmap，默认探测端口1-1024，-P参数可自定义端口范围
      1. -sP：使用ICMP协议，有点方便，快捷
      2. -sS：使用TCP半连接，优点速度快
      3. -sT：使用TCP全连接，优点准确可靠
      4. -sU：使用UDP协议，优点是可能透过防火墙，Linux下回特别慢，原因是Linux内核对于单位时间内收到icmp不可达的数目做了限制

演示使用宿主机的ip：10.203.4.235，对128使用该命令结果不明显，原因不明



* 1. ncat（瑞士军刀）
     1. -wX：X代表超时时间
     2. -z：输入输出
     3. -v：可视