nmap --iflist (查看本地路由与接口)

nmap -e 08:00:24:47:63:E6 103.10.87.478(指定mac和ip地址)

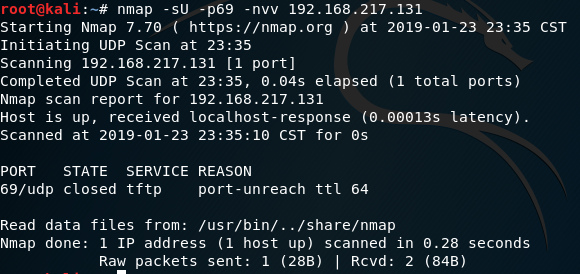
nmap -T4 -F -n -Pn -D192.168.1.100,192.168.1.101,192.168.1.102,ME192.168.1.103(地址诱骗)

nmap -sV --spoof-mac 08:00:27:47:63:E6 103.10.87.148(虚假mac地址)

nmap -sV --source-port 900 103.10.87.148 --source-port(指定源端口)

nmap -p1-25,80,512-515,2001,4001,6001,9001 10.20.0.1/16(扫描思科路由器)

nmap -sU -p69 -nvv 192.168.1.253(扫描路由器的tftp协议)



nmap -O -F -n 103.10.87.148 (-F快速扫描)

nmap -iR 100000 -sS -PS80 -p 445 -oG nmap.txt(随机产生10万个ip地址，对其445端口进行扫描。将扫描的结果以greppable(可用grep命令提取)格式输出到nmap.txt文件。

可以使用grep命令从输出文件提取关心的细节信息