1. nmap -sT 192.168.96.4 //TCP连接扫描，不安全，慢

2. nmap -sS 192.168.96.4 //SYN扫描,使用最频繁，安全，快

3. nmap -Pn 192.168.96.4 //目标机禁用ping，绕过ping扫描

4. nmap -sU 192.168.96.4 //UDP扫描,慢,可得到有价值的服务器程序

5. nmap -sI 僵尸ip 目标ip //使用僵尸机对目标机发送数据包

-S <IP\_Address>：伪造源地址

-sI 僵尸机扫描

6. nmap -sA 192.168.96.4 //检测哪些端口被屏蔽

7. nmap 192.168.96.4 -p <portnumber> //对指定端口扫描

8. nmap 192.168.96.1/24 //对整个网段的主机进行扫描

9. nmap 192.168.96.4 -oX myscan.xml //对扫描结果另存在myscan.xml

10. nmap -T1~6 192.168.96.4 //设置扫描速度，一般T4足够。

11. nmap -sV 192.168.96.4 //对端口上的服务程序版本进行扫描

12. nmap -O 192.168.96.4 //对目标主机的操作系统进行扫描

13. nmap -sC <scirptfile> 192.168.96.4 //使用脚本进行扫描，耗时长

14. nmap -A 192.168.96.4 //强力扫描，耗时长

15. nmap -6 ipv6地址 //对ipv6地址的主机进行扫描

16. nmap -f 192.168.96.4 //使用小数据包发送，避免被识别出

17. nmap –mtu <size> 192.168.96.4 //发送的包大小,最大传输单元必须是8的整数

18. nmap -D <假ip> 192.168.96.4 //发送参杂着假ip的数据包检测

19. nmap --source-port <portnumber> //针对防火墙只允许的源端口

20. nmap –data-length: <length> 192.168.96.4 //改变发生数据包的默认的长度，避免被识别出来是nmap发送的。

21. nmap -v 192.168.96.4 //显示冗余信息(扫描细节)

22. nmap -sn 192.168.96.4 //对目标进行ping检测，不进行端口扫描（会发送四种报文确定目标是否存活,）

23. nmap -sP 192.168.96.4 //仅仅对目标进行ping检测。

24. nmap -n/-p 192.168.96.4 //-n表示不进行dns解析，-p表示要

25. nmap --system-dns 192.168.96.4 //扫描指定系统的dns服务器

26. nmap –traceroute 192.168.96.4 //追踪每个路由节点。

27. nmap -PE/PP/PM: 使用ICMP echo, timestamp, and netmask 请求包发现主机。

28. nmap -sP 192.168.96.4 //主机存活性扫描，arp直连方式。

29. nmap -iR [number] //对随机生成number个地址进行扫描。

****Open****开放状态：

nmap 发起两个 SYN 的请求，服务器上监听在此端口的进程会进行应答，会返回 SYN/ACK， nmap 收到服务端返还回来的应答后会发送两个 RST ，并不会和服务端建立通信连接，完成端口的探测。

****Closed****关闭状态：

nmap 发起两个 SYN 的请求，服务器上由于没有进程监听该端口，内核会返回 RST， nmap 收到服务端返还回来的 RST 报文，将探测结果定义为 closed 。

****Filtered****过滤状态：

这种情况是服务端将收到的 nmap SYN 报文直接丢弃，不进行应答， 由于 nmap 直接发送了两个 SYN 报文，都没有收到应答，所以认定服务端开启了防火墙，将 SYN 报文丢弃。

Unfiltered 未过滤状态：

nmap 默认进行的是 SYN 扫描，当用 -sA 选项（ TCP ACK 扫描），连续发送两个同样的 ACK 报文，由于 snmp 确认收到了一个服务端根本没有发送的报文，所以服务端会发送一个 RST 报文， snmp 收到服务端发送来的 RST 报文后，确认服务端没有对报文进行丢弃处理，注意本探测不能发现端口是开放还是关闭状态，只能确认探测的报文服务端已收到，并回复给了 snmp RST报文。

****Open|filtered**** 开放或过滤状态：

这种状态主要是 nmap 无法区别端口处于 open 状态还是 filtered 状态。这种状态长出现于 UDP 端口，这种状态是服务端对 nmap 的请求不做任何回应，导致 nmap 无法确认端口是那种状态。

****Closed|filtered**** 关闭或者过滤状态：