第一种：Intense scan

(nmap -T4 -A -v)

一般来说，Intense scan 可以满足一般扫描

-T4 加快执行速度

-A 操作系统及版本探测

-v 显示详细的输出

第二种：Intense scan plus UDP

(nmap -sS -sU -T4 -A -v)

即 UDP 扫描

-sS TCP SYN 扫描

-sU UDP 扫描

第三种：Intense scan,all TCP ports

(nmap -p 1-65536 -T4 -A -v)

扫描所有 TCP 端口，范围在 1-65535，试图扫描所有端口的开放情况，速度比较慢。

-p 指定端口扫描范围

第四种：Intense scan,no ping

(nmap -T4 -A -v -Pn)

非 ping 扫描

-Pn 非 ping 扫描

第五种：Ping scan

(nmap -sn)

Ping 扫描

优点：速度快。

缺点：容易被防火墙屏蔽，导致无扫描结果

-sn ping 扫描

第六种：Quick scan

(nmap -T4 -F)

快速的扫描

-F 快速模式。

第七种：Quick scan plus

(nmap -sV -T4 -O -F --version-light)

快速扫描加强模式

-sV 探测端口及版本服务信息。

-O 开启 OS 检测

--version-light 设定侦测等级为 2。

第八种：Quick traceroute

(nmap -sn --traceroute)

路由跟踪

-sn Ping 扫描，关闭端口扫描

-traceroute 显示本机到目标的路由跃点。

第九种：Regular scan

规则扫描

第十种：Slow comprehensive scan

(nmap -sS -sU -T4 -A -v -PE -PP -PS80,443,-PA3389,PU40125 -PY -g 53 --script all)

慢速全面扫描。