Nmap最著名的功能之一是用TCP/IP协议栈fingerprinting进行远程操作系统探测。 Nmap发送一系列TCP和UDP报文到远程主机，检查响应中的每一个比特。 在进行一打测试如TCP ISN采样，TCP选项支持和排序，IPID采样，和初始窗口大小检查之后， Nmap把结果和数据库nmap-os-fingerprints中超过 1500个已知的操作系统的fingerprints进行比较，如果有匹配，就打印出操作系统的详细信息。 每个fingerprint包括一个自由格式的关于OS的描述文本， 和一个分类信息，它提供供应商名称(如Sun)，下面的操作系统(如Solaris)，OS版本(如10)， 和设备类型(通用设备，路由器，switch，游戏控制台， 等)。

nmap -sT -O 103.10.87.148

nmap -sT -p 3390 -O --osscan-limit 103.10.87.148

nmap -sA -O 103.10.87.148

-O (启用操作系统检测)

也可以使用-A来同时启用操作系统检测和版本检测。

- -osscan-limit (针对指定的目标进行操作系统检测)

如果发现一个打开和关闭的TCP端口时，操作系统检测会更有效。 采用这个选项，Nmap只对满足这个条件的主机进行操作系统检测，这样可以 节约时间，特别在使用-P0扫描多个主机时。这个选项仅在使用 -O或-A 进行操作系统检测时起作用。

- -osscan-guess; –fuzzy (推测操作系统检测结果)

当Nmap无法确定所检测的操作系统时，会尽可能地提供最相近的匹配，Nmap默认 进行这种匹配，使用上述任一个选项使得Nmap的推测更加有效。