

在 Nmap 中提供了很多扫描的方式，其中就有 ping 扫描方式，ping 扫描只进行 ping，然后显示出在线的主机。扫描时只需要加入 -sP 选项就可以启用 ping 扫描。

Nmap -sP 目标

优点：使用 ping 扫描可以轻易的获取目标信息而不会被轻易发现。在默认情况下，Nmap 会发送一个 ICMP 回声请求和一个 TCP 报文到目标端口。这是一种非常高效的扫描方式。