# 主机扫描

nmap -sL 103.10.87.1-255

nmap -PE 103.10.87.1-255

nmap -PS80 103.10.87.1-255

nmap -PR 192.168.1.1-255

nmap -Pn 103.10.87.1-255

nmap -sP 103.10.87.1-255

-P\*选项(用于选择 ping的类型)可以被结合使用。 您可以通过使用不同的TCP端口/标志位和ICMP码发送许多探测报文 来增加穿透防守严密的防火墙的机会。另外要注意的是即使您指定了其它 -P\*选项，ARP发现(-PR)对于局域网上的 目标而言是默认行为，因为它总是更快更有效。

下列选项控制主机发现。

-sL (列表扫描)

列表扫描是主机发现的退化形式，它仅仅列出指定网络上的每台主机， 不发送任何报文到目标主机。默认情况下，Nmap仍然对主机进行反向域名解析以获取 它们的名字。简单的主机名能给出的有用信息常常令人惊讶。例如， fw.chi.playboy.com是花花公子芝加哥办公室的 防火墙。Nmap最后还会报告IP地址的总数。列表扫描可以很好的确保您拥有正确的目标IP。 如果主机的域名出乎您的意料，那么就值得进一步检查以防错误地扫描其它组织的网络。

既然只是打印目标主机的列表，像其它一些高级功能如端口扫描，操作系统探测或者Ping扫描 的选项就没有了。如果您希望关闭ping扫描而仍然执行这样的高级功能，请继续阅读关于 -P0选项的介绍。

-sP (Ping扫描)

该选项告诉Nmap仅仅 进行ping扫描 (主机发现)，然后打印出对扫描做出响应的那些主机。 没有进一步的测试 (如端口扫描或者操作系统探测)。 这比列表扫描更积极，常常用于 和列表扫描相同的目的。它可以得到些许目标网络的信息而不被特别注意到。 对于攻击者来说，了解多少主机正在运行比列表扫描提供的一列IP和主机名往往更有价值。

系统管理员往往也很喜欢这个选项。 它可以很方便地得出 网络上有多少机器正在运行或者监视服务器是否正常运行。常常有人称它为 地毯式ping，它比ping广播地址更可靠，因为许多主机对广播请求不响应。

-sP选项在默认情况下， 发送一个ICMP回声请求和一个TCP报文到80端口。如果非特权用户执行，就发送一个SYN报文 (用connect()系统调用)到目标机的80端口。 当特权用户扫描局域网上的目标机时，会发送ARP请求(-PR)， ，除非使用了--send-ip选项。 -sP选项可以和除-P0)之外的任何发现探测类型-P\* 选项结合使用以达到更大的灵活性。 一旦使用了任何探测类型和端口选项，默认的探测(ACK和回应请求)就被覆盖了。 当防守严密的防火墙位于运行Nmap的源主机和目标网络之间时， 推荐使用那些高级选项。否则，当防火墙捕获并丢弃探测包或者响应包时，一些主机就不能被探测到。

-P0 -Pn (无ping,适合internet)

该选项完全跳过Nmap发现阶段。 通常Nmap在进行高强度的扫描时用它确定正在运行的机器。 默认情况下，Nmap只对正在运行的主机进行高强度的探测如 端口扫描，版本探测，或者操作系统探测。用-P0禁止 主机发现会使Nmap对每一个指定的目标IP地址 进行所要求的扫描。所以如果在命令行指定一个B类目标地址空间(/16)， 所有 65,536 个IP地址都会被扫描。 -P0的第二个字符是数字0而不是字母O。 和列表扫描一样，跳过正常的主机发现，但不是打印一个目标列表， 而是继续执行所要求的功能，就好像每个IP都是活动的。

-PS [portlist] (TCP SYN Ping)

该选项发送一个设置了SYN标志位的空TCP报文。 默认目的端口为80 (可以通过改变nmap.h) 文件中的DEFAULT-TCP-PROBE-PORT值进行配置，但不同的端口也可以作为选项指定。 甚至可以指定一个以逗号分隔的端口列表(如 -PS22，23，25，80，113，1050，35000)， 在这种情况下，每个端口会被并发地扫描。

SYN标志位告诉对方您正试图建立一个连接。 通常目标端口是关闭的，一个RST (复位) 包会发回来。 如果碰巧端口是开放的，目标会进行TCP三步握手的第二步，回应 一个SYN/ACK TCP报文。然后运行Nmap的机器则会扼杀这个正在建立的连接， 发送一个RST而非ACK报文，否则，一个完全的连接将会建立。 RST报文是运行Nmap的机器而不是Nmap本身响应的，因为它对收到 的SYN/ACK感到很意外。

Nmap并不关心端口开放还是关闭。 无论RST还是SYN/ACK响应都告诉Nmap该主机正在运行。

在UNIX机器上，通常只有特权用户 root 能否发送和接收 原始的TCP报文。因此作为一个变通的方法，对于非特权用户， Nmap会为每个目标主机进行系统调用connect()，它也会发送一个SYN 报文来尝试建立连接。如果connect()迅速返回成功或者一个ECONNREFUSED 失败，下面的TCP堆栈一定已经收到了一个SYN/ACK或者RST，该主机将被 标志位为在运行。 如果连接超时了，该主机就标志位为down掉了。这种方法也用于IPv6 连接，因为Nmap目前还不支持原始的IPv6报文。

-PA [portlist] (TCP ACK Ping)

TCP ACK ping和刚才讨论的SYN ping相当类似。 也许您已经猜到了，区别就是设置TCP的ACK标志位而不是SYN标志位。 ACK报文表示确认一个建立连接的尝试，但该连接尚未完全建立。 所以远程主机应该总是回应一个RST报文， 因为它们并没有发出过连接请求到运行Nmap的机器，如果它们正在运行的话。

-PA选项使用和SYN探测相同的默认端口(80)，也可以 用相同的格式指定目标端口列表。如果非特权用户尝试该功能， 或者指定的是IPv6目标，前面说过的connect()方法将被使用。 这个方法并不完美，因为它实际上发送的是SYN报文，而不是ACK报文。

提供SYN和ACK两种ping探测的原因是使通过防火墙的机会尽可能大。 许多管理员会配置他们的路由器或者其它简单的防火墙来封锁SYN报文，除非 连接目标是那些公开的服务器像公司网站或者邮件服务器。 这可以阻止其它进入组织的连接，同时也允许用户访问互联网。 这种无状态的方法几乎不占用防火墙/路由器的资源，因而被硬件和软件过滤器 广泛支持。Linux Netfilter/iptables 防火墙软件提供方便的 --syn选项来实现这种无状态的方法。 当这样的无状态防火墙规则存在时，发送到关闭目标端口的SYN ping探测 (-PS) 很可能被封锁。这种情况下，ACK探测格外有闪光点，因为它正好利用了 这样的规则。

另外一种常用的防火墙用有状态的规则来封锁非预期的报文。 这一特性已开始只存在于高端防火墙，但是这些年类它越来越普遍了。 Linux Netfilter/iptables 通过 --state选项支持这一特性，它根据连接状态把报文 进行分类。SYN探测更有可能用于这样的系统，由于没头没脑的ACK报文 通常会被识别成伪造的而丢弃。解决这个两难的方法是通过即指定 -PS又指定-PA来即发送SYN又发送ACK。

-PU [portlist] (UDP Ping)

还有一个主机发现的选项是UDP ping，它发送一个空的(除非指定了--data-length UDP报文到给定的端口。端口列表的格式和前面讨论过的-PS和-PA选项还是一样。 如果不指定端口，默认是31338。该默认值可以通过在编译时改变nmap.h文件中的 DEFAULT-UDP-PROBE-PORT值进行配置。默认使用这样一个奇怪的端口是因为对开放端口 进行这种扫描一般都不受欢迎。

如果目标机器的端口是关闭的，UDP探测应该马上得到一个ICMP端口无法到达的回应报文。 这对于Nmap意味着该机器正在运行。 许多其它类型的ICMP错误，像主机/网络无法到达或者TTL超时则表示down掉的或者不可到达的主机。 没有回应也被这样解释。如果到达一个开放的端口，大部分服务仅仅忽略这个 空报文而不做任何回应。这就是为什么默认探测端口是31338这样一个 极不可能被使用的端口。少数服务如chargen会响应一个空的UDP报文， 从而向Nmap表明该机器正在运行。

该扫描类型的主要优势是它可以穿越只过滤TCP的防火墙和过滤器。 例如。我曾经有过一个Linksys BEFW11S4无线宽带路由器。默认情况下， 该设备对外的网卡过滤所有TCP端口，但UDP探测仍然会引发一个端口不可到达 的消息，从而暴露了它自己。

-PE; -PP; -PM (ICMP Ping Types)

除了前面讨论的这些不常见的TCP和UDP主机发现类型， Nmap也能发送世人皆知的ping 程序所发送的报文。Nmap发送一个ICMP type 8 (回声请求)报文到目标IP地址， 期待从运行的主机得到一个type 0 (回声响应)报文。 对于网络探索者而言，不幸的是，许多主机和 防火墙现在封锁这些报文，而不是按期望的那样响应， 参见RFC 1122。因此，仅仅ICMP扫描对于互联网上的目标通常是不够的。 但对于系统管理员监视一个内部网络，它们可能是实际有效的途径。 使用-PE选项打开该回声请求功能。

虽然回声请求是标准的ICMP ping查询， Nmap并不止于此。ICMP标准 (RFC 792)还规范了时间戳请求，信息请求 request，和地址掩码请求，它们的代码分别是13，15和17。 虽然这些查询的表面目的是获取信息如地址掩码和当前时间， 它们也可以很容易地用于主机发现。 很简单，回应的系统就是在运行的系统。Nmap目前没有实现信息请求报文， 因为它们还没有被广泛支持。RFC 1122 坚持 “主机不应该实现这些消息”。 时间戳和地址掩码查询可以分别用-PP和-PM选项发送。 时间戳响应(ICMP代码14)或者地址掩码响应(代码18)表示主机在运行。 当管理员特别封锁了回声请求报文而忘了其它ICMP查询可能用于 相同目的时，这两个查询可能很有价值。

-PR (ARP Ping)

最常见的Nmap使用场景之一是扫描一个以太局域网。 在大部分局域网上，特别是那些使用基于 RFC1918私有地址范围的网络，在一个给定的时间绝大部分 IP地址都是不使用的。 当Nmap试图发送一个原始IP报文如ICMP回声请求时， 操作系统必须确定对应于目标IP的硬件 地址(ARP)，这样它才能把以太帧送往正确的地址。 这一般比较慢而且会有些问题，因为操作系统设计者认为一般不会在短时间内 对没有运行的机器作几百万次的ARP请求。

当进行ARP扫描时，Nmap用它优化的算法管理ARP请求。 当它收到响应时， Nmap甚至不需要担心基于IP的ping报文，既然它已经知道该主机正在运行了。 这使得ARP扫描比基于IP的扫描更快更可靠。 所以默认情况下，如果Nmap发现目标主机就在它所在的局域网上，它会进行ARP扫描。 即使指定了不同的ping类型(如 -PI或者 -PS) ，Nmap也会对任何相同局域网上的目标机使用ARP。 如果您真的不想要ARP扫描，指定 --send-ip。

-n (不用域名解析)

告诉Nmap 永不对它发现的活动IP地址进行反向域名解析。 既然DNS一般比较慢，这可以让事情更快些。

-R (为所有目标解析域名)

告诉Nmap 永远 对目标IP地址作反向域名解析。 一般只有当发现机器正在运行时才进行这项操作。

--system-dns (使用系统域名解析器)

默认情况下，Nmap通过直接发送查询到您的主机上配置的域名服务器 来解析域名。为了提高性能，许多请求 (一般几十个 ) 并发执行。如果您希望使用系统自带的解析器，就指定该选项 (通过getnameinfo()调用一次解析一个IP)。除非Nmap的DNS代码有bug--如果是这样，请联系我们。 一般不使用该选项，因为它慢多了。系统解析器总是用于IPv6扫描。

（3）-sA

nmap 10.0.1.161 -sA （发送tcp的ack包进行探测，可以探测主机是否存活）

【参数】

-sn 只探测存活主机，不扫描其他信息

eg:

nmap -Pn -sn 103.10.87.1-255