没有魔杖（或期权的 Nmap）承认或绕过防火墙或入侵检测系统。这项活动是需要技巧和经验。阿教程是超出了这些准则的意图，只列出了相关的选项，并描述他们做什么。

-f (分片报文); –mtu (使用指定的最小传输单元 – "MTU")的 MTU

使用- f 选项会强制扫描（还 "ping 扫描"）分段的 IP 数据包的使用。其基本思路是分裂了几包的 TCP 头，为了使包过滤器很难，一个 IDS 或与其他任务的理解发生了什么烦恼。然而，随后又非常小心使用此选项！有些方案微小的数据包处理这些问题。旧工具 "Sniffit" 将分割后故障立刻接收到第一个片段。指定此选项后`Nmap 的分裂成集的数据包最多 8 每个字节，在 IP 头后插入。这样，一个 TCP 头 20 字节会被分成三个包：两个八字节，并与其余四一。当然，每个片段也有 IP 头。重新指定- f 选项将用于套 16 字节（`从而减少碎片数量）。另外，您可以指定偏移（"抵销"）大小的选项 –mtu。不要使用- f 选项，如果它是用来 –mt 的 MTU 偏移量必须是一个倍数 8。虽然零散数据包将不会得到数据包过滤器和防火墙的队列中的所有 IP 分片（比如 GNU / Linux 机器已在内核 CONFIG_IP_ALWAYS_DEFRAG 选项），一些网络不能负担这将导致性能下降，从而给它启用。其他人无法启用，因为碎片可能采取不同的方向一旦进入。源系统整理一些在内核中传出的数据包。Linux 模块 ip_conntrack 的金正日（"连接跟踪模块"）就是其中之一。建议而嗅探器扫描（来虚灵）正在转向，以确保发送的数据包碎片。如果你的操作系统是造成这个问题，使用该选项 –send_eth 绕过 IP 层和原始以太网帧发送。

-ð (形成一个扫描使用诱饵 – "诱饵扫描")

这个选项要求在 "诱饵扫描"（或使用诱饵扫描）在目标主机会显示为诱饵，从指定的主机为未来的眼睛。在这种方式，IDS 将显示目标网络 5-10 唯一的 IP 地址从端口扫描，他们不会知道什么是真正的 IP 攻击源的 IP 是什么只是作为掩蔽使用。虽然这可以被击败通过路由器所采取的路由跟踪（"路由器路径追踪"），响应下降，以及其他活动的机制，一般用于隐藏自己的 IP 地址的有效方法。

用逗号分隔每个诱饵主机，并且可以使用作为一个诱饵我代表您的 IP 地址的位置。如果您能在第六位 ME 或更高，一些常见的端口扫描探测器（作为优秀的 "scanlogd" 太阳能设计师）不会显示您的 IP 地址。如果你用我，Nmap 是意志把你一个随机的位置。

请注意，您作为诱饵的主机使用，否则你应该建立一个运行风险 "SYN 泛滥" 你的目标。同时这将是很容易确定哪个主机的事业扫描，如果只有一个是在网络中活跃。这是建议使用的名称而不是 IP 地址，以防止其企图诱骗网络的 DNS 名称解析的日志中。

无论是在使用诱饵 "ping 扫描" 首页（不管你是否使用 ICMP, SYN 的，应答，等）无论是在实际的扫描端口。诱饵也可用于在 "作业系统检测" 远程，指定的- O）。你的诱饵使用不正确的类型的扫描 "版本检测" 或 TCP 连接扫描()。

不用说，使用太多的诱饵可能会降低您的扫描，并可能使其不准确。此外，一些互联网服务供应商（“互联网服务供应商”）可以过滤数据包“欺骗”（伪造），虽然很多人对后者无法运行任何类型的行动。
-S (falsifica l'indirizzo sorgente – “源地址欺骗”)

在某些情况下，**Nmap** 还可能无法确定你的源地址（**Nmap** 会告诉你在这些情况下这个问题`）。在这种情况下，如果你能使用的 **IP** 接口的，是你要发送的数据包。

这个选项的另一个可能的应用是伪造（“欺骗”）扫描到的目标是针对有人认为他们是对他们做扫描。想象会发生什么，如果一家公司只有被认识到的猎物从他们的竞争对手端口扫描！的，而且它一般是为这个特定用途所需的选项，而且还建议使用-求解 **P0.**
-和（使用指定的网络接口 – “使用指定的接口”)

告诉 **Nmap** 网络接口，用于发送和接收数据包。**Nmap** 软件应该能够看到自己使用，但如果你不能告诉你，如果你`。
–源端口
; -克
(记下的源端口号欺骗)

令人惊讶的是一个普通的配置只有在信任基础的流量源端口。这是很容易看到这都：管理员设置了一个全新的防火墙，只有被从用户的应用忘恩负义抱怨充斥停止工作。例如，**DNS** 查询不破，因为答案'（**UDP** 数据包的形式）从外部服务器无法再进入网络。此外 **FTP** 是另一个常见的　　例子：活跃　　在数据传输（反对那些类型“被动 **FTP**”）远程服务器试图建立与客户直接连接来传输所需的文件。

对于这些问题，安全的解决办法，通常在应用程序级代理防火墙模块或议定书的形式，解析。不幸的是，也更容易，不安全的解决方案。例如，注意到从端口来的 **DNS** 回复 **53** 荣传输的 **FTP** “活跃” 从端口 **20**，许多经理人落入陷阱，简单地允许从这些端口传入的通信。他们通常认为任何攻击者会注意到这些安全漏洞和 **appprofittarne**。在其他情况下，管理员可能会考虑这个解决方案是一项临时措施，直到他们可以实现一个更美好，更安全。然后你忘了做。

有太多的事情做的是网络管理员并非只有落入这个圈套。许多产品都带有这些不安全规则；即使微软已经认罪。适用于 **Windows** 的 **IPsec** 筛选器 **2000** 和 **Windows XP** 包含一个隐含的规则，允许从所有港口的交通通道 **88 (Kerberos** 的）。另一个区域警报个人防火墙著名案例（到版本 **2.1.25:** 它允许进入的 **UDP** 数据包的任何系统，作为其源已进港 **53 (DNS** 的）的 **67 (**的 **DHCP).**

Nmap 提供选项（等效）**-**克 –源端口利用这些弱点。只需提供一个端口号和 **Nmap** 会从该端口发送数据包在可能。但是 **Nmap** 的操作系统必须使用某些检测试验不同的端口号才能正常工作，因为`，**DNS** 请求，而忽略的选项 –源端口旗因为 **Nmap** 依赖于系统库管理。大多数 **TCP** 扫描，包括 **SYN** 和 **UDP** 扫描，支持选项。

–数据长度（随机数据添加到发送的数据包）

Nmap 发送通常在最小的可能大小更多的数据包，只包含头（头）. 因此，它通常是 TCP 包 40 字节和 ICMP 回应请求 28 字节. 此选项告诉 Nmap 追加给定数目的随机字节几乎所有的数据包发送. 检测的操作系统软件包，但是，都没有改变，为什么在他们的精度要求在探头发送某种一致性; 然而，在几乎所有的选项和端口扫描屏支持这种模式`. 它会降低性能，而且可以在更准确的结果扫描.

–TTL 电（设置 IP 的时间到现场）

设定时间现场到现场（一生的 IPv4 数据包）为所需的值.

–随机东道主（随机的顺序目标主机）

此选项告诉 Nmap 扫描主机洗牌每个组（到 8096）在开始扫描. 这可以使在不同的网络监控系统的扫描，尤其是当你结合它的选项放缓（“慢的时间”）. 如果你想在大组随机尺寸，要加大对 PING_GROUP_SZ nmap.h 指令重新编译应用程序. 另一种解决办法是将产生的 IP 列表上能够通过扫描它扫描列表（- SL 的- N 的上 ），随机与一个 Perl 脚本，并通过列表的 Nmap 与金正日.

–欺骗和 MAC (制作的硬件欺骗（陆委会))

Nmap 的使用要求的硬件地址（苹果）所有的原始以太网帧中发送. Quest'opzione 意味着 –的发送，以确保联邦理工学院 Nmap 的实际发送以太网数据包级. 陆委会可以指定各种格式: 这里是字符串“0”，为本届会议的 Nm ap 选择一个完全随机的 MAC. 如果字符串是偶数的十六进制数字（可选的双冒号分隔），Nmap 的 UserA 的身份来的 MAC`questo. 指定不应该比 12 小数，Nmap 的填补了其余 6 字节的随机值. 如果参数不是一个零（0）或十六进制字符串，Nmap 的期待找到一个供应商名称包含给定的字符串，通过使用 nmap - MAC 的前缀（大写和小写之间没有区别）. 如果找到一个匹配，Nmap 的使用供应商的 OUI 的（前缀 3 字节）并填写其余 6 随机字节. 有效的使用范例 –欺骗，苹果的 Mac 索诺，0，01:02:03:04:05:06，deadbeefcafe，0020F2键，和思科.

–badsum (校验和的 TCP / UDP 发送数据包无效)

要求 Nmap 使用的数据包发送到目标主机的 TCP 或 UDP 校验和无效. 因为几乎所有主机的 IP 堆栈适当降最终将这些数据包，任何收到的答复很可能受到防火墙或入侵检测系统（入侵检测系统）也懒得去验证校验