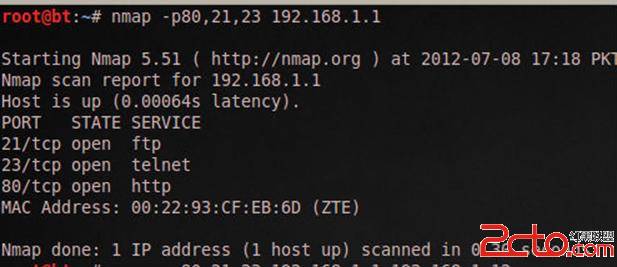
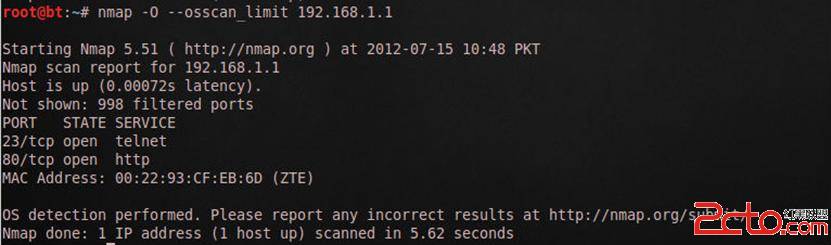
**渗透测试工具Nmap从初级到高级使用教程**

2012-07-24      [个评论](http://www.2cto.com/Article/201207/142903.html#SOHUCS)       作者：[阿德马](http://space.2cto.com/nxadmin)

[收藏](javascript:;)    [[http://www.2cto.com/statics/images/dl.jpg](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)我要投稿](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)

本文由阿德马翻译自国外网站，请尊重劳动成果，转载请注明出处，谢谢  
   
Nmap是一款网络扫描和主机检测的非常有用的工具。Nmap是不局限于仅仅收集信息和枚举，同时可以用来作为一个漏洞探测器或安全扫描器。它可以适用于winodws,linux,mac等操作系统。Nmap是一款非常强大的实用工具,可用于：  
   
检测活在网络上的主机（主机发现）  
检测主机上开放的端口（端口发现或枚举）  
检测到相应的端口（服务发现）的软件和版本  
检测操作系统，硬件地址，以及软件版本  
检测脆弱性的漏洞（Nmap的脚本）  
Nmap是一个非常普遍的工具，它有命令行界面和图形用户界面。本人包括以下方面的内容:  
   
介绍Nmap  
   
扫描中的重要参数  
   
操作系统检测  
   
Nmap使用教程  
   
Nmap使用不同的技术来执行扫描，包括：TCP的connect（）扫描，TCP反向的ident扫描，FTP反弹扫描等。所有这些扫描的类型有自己的优点和缺点，我们接下来将讨论这些问题。  
   
Nmap的使用取决于目标主机,因为有一个简单的（基本）扫描和预先扫描之间的差异。我们需要使用一些先进的技术来绕过防火墙和入侵检测/防御系统，以获得正确的结果。下面是一些基本的命令和它们的用法的例子：  
   
扫描单一的一个主机，命令如下：  
   
#nmap nxadmin.com  
   
#nmap 192.168.1.2  
   
扫描整个子网,命令如下:  
   
#nmap 192.168.1.1/24  
   
扫描多个目标,命令如下：  
   
#nmap 192.168.1.2 192.168.1.5  
   
扫描一个范围内的目标,如下：  
   
#nmap 192.168.1.1-100 (扫描IP地址为192.168.1.1-192.168.1.100内的所有主机)  
   
如果你有一个ip地址列表，将这个保存为一个txt文件，和namp在同一目录下,扫描这个txt内的所有主机，命令如下：  
   
#nmap -iL target.txt  
   
如果你想看到你扫描的所有主机的列表，用以下命令:  
   
#nmap -sL 192.168.1.1/24  
   
扫描除过某一个ip外的所有子网主机,命令：  
   
#nmap 192.168.1.1/24 -exclude 192.168.1.1  
   
扫描除过某一个文件中的ip外的子网主机命令  
   
#nmap 192.168.1.1/24 -exclude file xxx.txt  (xxx.txt中的文件将会从扫描的主机中排除)  
   
扫描特定主机上的80,21,23端口,命令如下  
   
#nmap -p80,21,23 192.168.1.1  
   
   
  
   
从上面我们已经了解了Nmap的基础知识，下面我们深入的探讨一下Nmap的扫描技术.  
   
Tcp SYN Scan (sS)  
   
这是一个基本的扫描方式,它被称为半开放扫描，因为这种技术使得Nmap不需要通过完整的握手，就能获得远程主机的信息。Nmap发送SYN包到远程主机，但是它不会产生任何会话.因此不会在目标主机上产生任何日志记录,因为没有形成会话。这个就是SYN扫描的优势.  
   
如果Nmap命令中没有指出扫描类型,默认的就是Tcp SYN.但是它需要root/administrator权限.  
   
#nmap -sS 192.168.1.1  
   
Tcp connect() scan(sT)  
   
如果不选择SYN扫描,TCP connect()扫描就是默认的扫描模式.不同于Tcp SYN扫描,Tcp connect()扫描需要完成三次握手,并且要求调用系统的connect().Tcp connect()扫描技术只适用于找出TCP和UDP端口.  
   
#nmap -sT 192.168.1.1  
   
Udp scan(sU)  
   
顾名思义,这种扫描技术用来寻找目标主机打开的UDP端口.它不需要发送任何的SYN包，因为这种技术是针对UDP端口的。UDP扫描发送UDP数据包到目标主机，并等待响应,如果返回ICMP不可达的错误消息，说明端口是关闭的，如果得到正确的适当的回应，说明端口是开放的.  
   
#nmap -sU 192.168.1.1  
   
FIN scan (sF)  
   
有时候Tcp SYN扫描不是最佳的扫描模式,因为有防火墙的存在.目标主机有时候可能有IDS和IPS系统的存在,防火墙会阻止掉SYN数据包。发送一个设置了FIN标志的数据包并不需要完成TCP的握手.  
   
root@bt:~# nmap -sF 192.168.1.8  
   
Starting Nmap 5.51  at 2012-07-08 19:21 PKT  
   
Nmap scan report for 192.168.1.8  
   
Host is up (0.000026s latency).  
   
Not shown: 999 closed ports  
   
PORT STATE SERVICE  
   
111/tcp open|filtered rpcbind  
   
FIN扫描也不会在目标主机上创建日志(FIN扫描的优势之一).个类型的扫描都是具有差异性的,FIN扫描发送的包只包含FIN标识,NULL扫描不发送数据包上的任何字节,XMAS扫描发送FIN、PSH和URG标识的数据包.  
   
PING Scan (sP)  
   
PING扫描不同于其它的扫描方式，因为它只用于找出主机是否是存在在网络中的.它不是用来发现是否开放端口的.PING扫描需要ROOT权限，如果用户没有ROOT权限,PING扫描将会使用connect()调用.  
   
#nmap -sP 192.168.1.1  
   
版本检测(sV)  
   
版本检测是用来扫描目标主机和端口上运行的软件的版本.它不同于其它的扫描技术，它不是用来扫描目标主机上开放的端口，不过它需要从开放的端口获取信息来判断软件的版本.使用版本检测扫描之前需要先用TCP SYN扫描开放了哪些端口.  
   
#nmap -sV 192.168.1.1  
   
Idle scan (sL)  
   
Idle scan是一种先进的扫描技术，它不是用你真实的主机Ip发送数据包，而是使用另外一个目标网络的主机发送数据包.  
   
#nmap -sL 192.168.1.6 192.168.1.1  
   
Idle scan是一种理想的匿名扫描技术,通过目标网络中的192.168.1.6向主机192.168.1.1发送数据，来获取192.168.1.1开放的端口  
   
有需要其它的扫描技术，如FTP bounce（FTP反弹）, fragmentation scan（碎片扫描）, IP protocol scan（IP协议扫描）,以上讨论的是几种最主要的扫描方式.  
   
Nmap的OS检测（O）  
   
Nmap最重要的特点之一是能够远程检测操作系统和软件，Nmap的OS检测技术在渗透测试中用来了解远程主机的操作系统和软件是非常有用的，通过获取的信息你可以知道已知的漏洞。Nmap有一个名为的nmap-OS-DB数据库，该数据库包含超过2600操作系统的信息。Nmap把TCP和UDP数据包发送到目标机器上，然后检查结果和数据库对照。  
   
Initiating SYN Stealth Scan at 10:21  
Scanning localhost (127.0.0.1) [1000 ports]  
Discovered open port 111/tcp on 127.0.0.1  
Completed SYN Stealth Scan at 10:21, 0.08s elapsed (1000 total ports)  
Initiating OS detection (try #1) against localhost (127.0.0.1)  
Retrying OS detection (try #2) against localhost (127.0.0.1)  
   
上面的例子清楚地表明，Nmap的首次发现开放的端口，然后发送数据包发现远程操作系统。操作系统检测参数是O（大写O）  
   
  
   
   
Nmap的操作系统指纹识别技术：  
   
设备类型（路由器，工作组等）  
运行（运行的操作系统）  
操作系统的详细信息（操作系统的名称和版本）  
网络距离（目标和攻击者之间的距离跳）  
   
如果远程主机有防火墙，IDS和IPS系统，你可以使用-PN命令来确保不ping远程主机，因为有时候防火墙会组织掉ping请求.-PN命令告诉Nmap不用ping远程主机。  
   
# nmap -O -PN 192.168.1.1/24  
   
以上命令告诉发信主机远程主机是存活在网络上的，所以没有必要发送ping请求,使用-PN参数可以绕过PING命令,但是不影响主机的系统的发现.  
   
Nmap的操作系统检测的基础是有开放和关闭的端口，如果OS scan无法检测到至少一个开放或者关闭的端口，会返回以下错误： [www.2cto.com](http://www.2cto.com/)  
   
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
   
OS Scan的结果是不可靠的，因为没有发现至少一个开放或者关闭的端口.  
   
   
   
  
  
   
   
这种情况是非常不理想的，应该是远程主机做了针对操作系统检测的防范。如果Nmap不能检测到远程操作系统类型，那么就没有必要使用-osscan\_limit检测。  
   
   
   
想好通过Nmap准确的检测到远程操作系统是比较困难的，需要使用到Nmap的猜测功能选项, –osscan-guess 猜测认为最接近目标的匹配操作系统类型。  
   
# nmap -O --osscan-guess 192.168.1.1  
   
总结  
   
Nmap是一个非常强大的工具，它具有覆盖[渗透](http://vip.2cto.com/Article/61.html)测试的第一方面的能力，其中包括信息的收集和统计。本文从初级到高级的讲解了Nmap入侵扫描工具的使用.希望对大家有所帮助.

摘要

　　nmap是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取那台主机正在运行以及提供什么服务等信息。nmap支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。从扫描类型一节可以得到细节。nmap还提供了一些高级的特征，例如：通过TCP/IP协议栈特征探测操作系统类型，秘密扫描，动态延时和重传计算，并行扫描，通过并行ping扫描探测关闭的主机，诱饵扫描，避开端口过滤检测，直接RPC扫描(无须端口影射)，碎片扫描，以及灵活的目标和端口设定.

--------------------------------------------------------------------------------

1.名称

nmap-网络探测和安全扫描工具

2.语法

nmap [Scan Type(s)] [Options]

3.描述

　　nmap是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取那台主机正在运行以及提供什么服务等信息。nmap支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。从扫描类型一节可以得到细节。nmap还提供了一些高级的特征，例如：通过TCP/IP协议栈特征探测操作系统类型，秘密扫描，动态延时和重传计算，并行扫描，通过并行ping扫描探测关闭的主机，诱饵扫描，避开端口过滤检测，直接RPC扫描(无须端口影射)，碎片扫描，以及灵活的目标和端口设定。

　　为了提高nmap在non-root状态下的性能，软件的设计者付出了很大的努力。很不幸，一些内核界面(例如raw socket)需要在root状态下使用。所以应该尽可能在root使用nmap。

　　nmap运行通常会得到被扫描主机端口的列表。nmap总会给出well known端口的服务名(如果可能)、端口号、状态和协议等信息。每个端口的状态有：open、filtered、unfiltered。open状态意味着目标主机能够在这个端口使用accept()系统调用接受连接。filtered状态表示：防火墙、包过滤和其它的网络安全软件掩盖了这个端口，禁止 nmap探测其是否打开。unfiltered表示：这个端口关闭，并且没有防火墙/包过滤软件来隔离nmap的探测企图。通常情况下，端口的状态基本都是unfiltered状态，只有在大多数被扫描的端口处于filtered状态下，才会显示处于unfiltered状态的端口。

　　根据使用的功能选项，nmap也可以报告远程主机的下列特征：使用的操作系统、TCP序列、运行绑定到每个端口上的应用程序的用户名、DNS名、主机地址是否是欺骗地址、以及其它一些东西。

4.功能选项

　　功能选项可以组合使用。一些功能选项只能够在某种扫描模式下使用。nmap会自动识别无效或者不支持的功能选项组合，并向用户发出警告信息。

　　如果你是有经验的用户，可以略过结尾的示例一节。可以使用nmap -h快速列出功能选项的列表。

4.1 扫描类型

　　-sT

　　TCP connect()扫描：这是最基本的TCP扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接。如果目标端口有程序监听， connect()就会成功返回，否则这个端口是不可达的。这项技术最大的优点是，你勿需root权限。任何UNIX用户都可以自由使用这个系统调用。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。

　　-sS

　　TCP同步扫描(TCP SYN)：因为不必全部打开一个TCP连接，所以这项技术通常称为半开扫描(half-open)。你可以发出一个TCP同步包(SYN)，然后等待回应。如果对方返回SYN|ACK(响应)包就表示目标端口正在监听；如果返回RST数据包，就表示目标端口没有监听程序；如果收到一个SYN|ACK包，源主机就会马上发出一个RST(复位)数据包断开和目标主机的连接，这实际上有我们的操作系统内核自动完成的。这项技术最大的好处是，很少有系统能够把这记入系统日志。不过，你需要root权限来定制SYN数据包。

　　-sF -sF -sN

　　秘密FIN数据包扫描、圣诞树(Xmas Tree)、空(Null)扫描模式：即使SYN扫描都无法确定的情况下使用。一些防火墙和包过滤软件能够对发送到被限制端口的SYN数据包进行监视，而且有些程序比如synlogger和courtney能够检测那些扫描。这些高级的扫描方式可以逃过这些干扰。这些扫描方式的理论依据是：关闭的端口需要对你的探测包回应RST包，而打开的端口必需忽略有问题的包(参考RFC 793第64页)。FIN扫描使用暴露的FIN数据包来探测，而圣诞树扫描打开数据包的FIN、URG和PUSH标志。不幸的是，微软决定完全忽略这个标准，另起炉灶。所以这种扫描方式对Windows95/NT无效。不过，从另外的角度讲，可以使用这种方式来分别两种不同的平台。如果使用这种扫描方式可以发现打开的端口，你就可以确定目标注意运行的不是Windows系统。如果使用-sF、-sX或者-sN扫描显示所有的端口都是关闭的，而使用SYN扫描显示有打开的端口，你可以确定目标主机可能运行的是Windwos系统。现在这种方式没有什么太大的用处，因为nmap有内嵌的操作系统检测功能。还有其它几个系统使用和windows同样的处理方式，包括Cisco、BSDI、HP/UX、MYS、IRIX。在应该抛弃数据包时，以上这些系统都会从打开的端口发出复位数据包。

　　-sP

　　ping扫描：有时你只是想知道此时网络上哪些主机正在运行。通过向你指定的网络内的每个IP地址发送ICMP echo请求数据包，nmap就可以完成这项任务。如果主机正在运行就会作出响应。不幸的是，一些站点例如：microsoft.com阻塞ICMP echo请求数据包。然而，在默认的情况下nmap也能够向80端口发送TCP ack包，如果你收到一个RST包，就表示主机正在运行。nmap使用的第三种技术是：发送一个SYN包，然后等待一个RST或者SYN/ACK包。对于非root用户，nmap使用connect()方法。

　　在默认的情况下(root用户)，nmap并行使用ICMP和ACK技术。

　　注意，nmap在任何情况下都会进行ping扫描，只有目标主机处于运行状态，才会进行后续的扫描。如果你只是想知道目标主机是否运行，而不想进行其它扫描，才会用到这个选项。

　　-sU

　　UDP扫描：如果你想知道在某台主机上提供哪些UDP(用户数据报协议,RFC768)服务，可以使用这种扫描方法。nmap首先向目标主机的每个端口发出一个0字节的UDP包，如果我们收到端口不可达的ICMP消息，端口就是关闭的，否则我们就假设它是打开的。

　　有些人可能会想UDP扫描是没有什么意思的。但是，我经常会想到最近出现的solaris rpcbind缺陷。rpcbind隐藏在一个未公开的UDP端口上，这个端口号大于32770。所以即使端口111(portmap的众所周知端口号) 被防火墙阻塞有关系。但是你能发现大于30000的哪个端口上有程序正在监听吗?使用UDP扫描就能！cDc Back Orifice的后门程序就隐藏在Windows主机的一个可配置的UDP端口中。不考虑一些通常的安全缺陷，一些服务例如:snmp、tftp、NFS 使用UDP协议。不幸的是，UDP扫描有时非常缓慢，因为大多数主机限制ICMP错误信息的比例(在RFC1812中的建议)。例如，在Linux内核中 (在net/ipv4/icmp.h文件中)限制每4秒钟只能出现80条目标不可达的ICMP消息，如果超过这个比例，就会给1/4秒钟的处罚。 solaris的限制更加严格，每秒钟只允许出现大约2条ICMP不可达消息，这样，使扫描更加缓慢。nmap会检测这个限制的比例，减缓发送速度，而不是发送大量的将被目标主机丢弃的无用数据包。

　　不过Micro$oft忽略了RFC1812的这个建议，不对这个比例做任何的限制。所以我们可以能够快速扫描运行Win95/NT的主机上的所有65K个端口。

　　-sA

　　ACK扫描：这项高级的扫描方法通常用来穿过防火墙的规则集。通常情况下，这有助于确定一个防火墙是功能比较完善的或者是一个简单的包过滤程序，只是阻塞进入的SYN包。

　　这种扫描是向特定的端口发送ACK包(使用随机的应答/序列号)。如果返回一个RST包，这个端口就标记为unfiltered状态。如果什么都没有返回，或者返回一个不可达ICMP消息，这个端口就归入filtered类。注意，nmap通常不输出unfiltered的端口，所以在输出中通常不显示所有被探测的端口。显然，这种扫描方式不能找出处于打开状态的端口。

　　-sW

　　对滑动窗口的扫描：这项高级扫描技术非常类似于ACK扫描，除了它有时可以检测到处于打开状态的端口，因为滑动窗口的大小是不规则的，有些操作系统可以报告其大小。这些系统至少包括：某些版本的AIX、Amiga、BeOS、BSDI、Cray、Tru64 UNIX、DG/UX、OpenVMS、Digital UNIX、OpenBSD、OpenStep、QNX、Rhapsody、SunOS 4.x、Ultrix、VAX、VXWORKS。从nmap-hackers邮件3列表的文档中可以得到完整的列表。

　　-sR

　　RPC扫描。这种方法和nmap的其它不同的端口扫描方法结合使用。选择所有处于打开状态的端口向它们发出SunRPC程序的NULL命令，以确定它们是否是RPC端口，如果是，就确定是哪种软件及其版本号。因此你能够获得防火墙的一些信息。诱饵扫描现在还不能和RPC扫描结合使用。

　　-b

　　FTP反弹攻击(bounce attack):FTP协议(RFC 959)有一个很有意思的特征，它支持代理FTP连接。也就是说，我能够从evil.com连接到FTP服务器target.com，并且可以要求这台 FTP服务器为自己发送Internet上任何地方的文件！1985年，RFC959完成时，这个特征就能很好地工作了。然而，在今天的Internet 中，我们不能让人们劫持FTP服务器，让它向Internet上的任意节点发送数据。如同Hobbit在1995年写的文章中所说的，这个协议"能够用来做投递虚拟的不可达邮件和新闻，进入各种站点的服务器,填满硬盘，跳过防火墙，以及其它的骚扰活动，而且很难进行追踪"。我们可以使用这个特征，在一台代理FTP服务器扫描TCP端口。因此，你需要连接到防火墙后面的一台FTP服务器，接着进行端口扫描。如果在这台FTP服务器中有可读写的目录，你还可以向目标端口任意发送数据(不过nmap不能为你做这些)。

　　传递给-b功能选项的参数是你要作为代理的FTP服务器。语法格式为：

　　-b username:password@server:port。

　　除了server以外，其余都是可选的。如果你想知道什么服务器有这种缺陷，可以参考我在Phrack 51发表的文章。还可以在nmap的站点得到这篇文章的最新版本。

4.2 通用选项

　　这些内容不是必需的，但是很有用。

　　-P0

　　在扫描之前，不必ping主机。有些网络的防火墙不允许ICMP echo请求穿过，使用这个选项可以对这些网络进行扫描。microsoft.com就是一个例子，因此在扫描这个站点时，你应该一直使用-P0或者-PT 80选项。

　　-PT

　　扫描之前，使用TCP ping确定哪些主机正在运行。nmap不是通过发送ICMP echo请求包然后等待响应来实现这种功能，而是向目标网络(或者单一主机)发出TCP ACK包然后等待回应。如果主机正在运行就会返回RST包。只有在目标网络/主机阻塞了ping包，而仍旧允许你对其进行扫描时，这个选项才有效。对于非 root用户，我们使用connect()系统调用来实现这项功能。使用-PT <端口号>来设定目标端口。默认的端口号是80，因为这个端口通常不会被过滤。

　　-PS

　　对于root用户，这个选项让nmap使用SYN包而不是ACK包来对目标主机进行扫描。如果主机正在运行就返回一个RST包(或者一个SYN/ACK包)。

　　-PI

　　设置这个选项，让nmap使用真正的ping(ICMP echo请求)来扫描目标主机是否正在运行。使用这个选项让nmap发现正在运行的主机的同时，nmap也会对你的直接子网广播地址进行观察。直接子网广播地址一些外部可达的IP地址，把外部的包转换为一个内向的IP广播包，向一个计算机子网发送。这些IP广播包应该删除，因为会造成拒绝服务攻击(例如 smurf)。

　　-PB

　　这是默认的ping扫描选项。它使用ACK(-PT)和ICMP(-PI)两种扫描类型并行扫描。如果防火墙能够过滤其中一种包，使用这种方法，你就能够穿过防火墙。

　　-O

　　这个选项激活对TCP/IP指纹特征(fingerprinting)的扫描，获得远程主机的标志。换句话说，nmap使用一些技术检测目标主机操作系统网络协议栈的特征。nmap使用这些信息建立远程主机的指纹特征，把它和已知的操作系统指纹特征数据库做比较，就可以知道目标主机操作系统的类型。

　　-I

　　这个选项打开nmap的反向标志扫描功能。Dave Goldsmith 1996年向bugtap发出的邮件注意到这个协议，ident协议(rfc 1413)允许使用TCP连接给出任何进程拥有者的用户名，即使这个进程并没有初始化连接。例如，你可以连接到HTTP端口，接着使用identd确定这个服务器是否由root用户运行。这种扫描只能在同目标端口建立完全的TCP连接时(例如：-sT扫描选项)才能成功。使用-I选项是，远程主机的 identd精灵进程就会查询在每个打开的端口上监听的进程的拥有者。显然，如果远程主机没有运行identd程序，这种扫描方法无效。

　　-f

　　这个选项使nmap使用碎片IP数据包发送SYN、FIN、XMAS、NULL。使用碎片数据包增加包过滤、入侵检测系统的难度，使其无法知道你的企图。不过，要慎重使用这个选项！有些程序在处理这些碎片包时会有麻烦，我最喜欢的嗅探器在接受到碎片包的头36个字节时，就会发生 segmentation faulted。因此，在nmap中使用了24个字节的碎片数据包。虽然包过滤器和防火墙不能防这种方法，但是有很多网络出于性能上的考虑，禁止数据包的分片。

　　注意这个选项不能在所有的平台上使用。它在Linux、FreeBSD、OpenBSD以及其它一些UNIX系统能够很好工作。

　　-v

　　冗余模式。强烈推荐使用这个选项，它会给出扫描过程中的详细信息。使用这个选项，你可以得到事半功倍的效果。使用-d选项可以得到更加详细的信息。

　　-h

　　快速参考选项。

　　-oN

　　把扫描结果重定向到一个可读的文件logfilename中。

　　-oM

　　把扫描结果重定向到logfilename文件中，这个文件使用主机可以解析的语法。你可以使用-oM -来代替logfilename，这样输出就被重定向到标准输出stdout。在这种情况下，正常的输出将被覆盖，错误信息荏苒可以输出到标准错误 stderr。要注意，如果同时使用了-v选项，在屏幕上会打印出其它的信息。

　　-oS 　　 thIs l0gz th3 r3suLtS of YouR ScanZ iN a s| 　　THe fiL3 U sPecfy 4s an arGuMEnT! U kAn gIv3 the 4rgument -

　　(wItHOUt qUOteZ) to sh00t output iNT0 stDouT!@!! 莫名其妙，下面是我猜着翻译的，相形字？

　　把扫描结果重定向到一个文件logfilename中，这个文件使用一种"hei客方言"的语法形式(作者开的玩笑?)。同样，使用-oS -就会把结果重定向到标准输出上。

　　-resume

　　某个网络扫描可能由于control-C或者网络损失等原因被中断，使用这个选项可以使扫描接着以前的扫描进行。logfilename是被取消扫描的日志文件，它必须是可读形式或者机器可以解析的形式。而且接着进行的扫描不能增加新的选项，只能使用与被中断的扫描相同的选项。nmap会接着日志文件中的最后一次成功扫描进行新的扫描。

　　-iL

　　从inputfilename文件中读取扫描的目标。在这个文件中要有一个主机或者网络的列表，由空格键、制表键或者回车键作为分割符。如果使用-iL -，nmap就会从标准输入stdin读取主机名字。你可以从指定目标一节得到更加详细的信息。

　　-iR

　　让nmap自己随机挑选主机进行扫描。

　　-p <端口范围>

　　这个选项让你选择要进行扫描的端口号的范围。例如，-p 23表示：只扫描目标主机的23号端口。-p 20-30,139,60000-表示：扫描20到30号端口，139号端口以及所有大于60000的端口。在默认情况下，nmap扫描从1到1024号以及nmap-services文件(如果使用RPM软件包，一般在/usr/share/nmap/目录中)中定义的端口列表。

　　-F

　　快速扫描模式，只扫描在nmap-services文件中列出的端口。显然比扫描所有65535个端口要快。

　　-D

　　使用诱饵扫描方法对目标网络/主机进行扫描。如果nmap使用这种方法对目标网络进行扫描，那么从目标主机/网络的角度来看，扫描就象从其它主机 (decoy1,等)发出的。从而，即使目标主机的IDS(入侵检测系统)对端口扫描发出报警，它们也不可能知道哪个是真正发起扫描的地址，哪个是无辜的。这种扫描方法可以有效地对付例如路由跟踪、response-dropping等积极的防御机制，能够很好地隐藏你的IP地址。

　　每个诱饵主机名使用逗号分割开，你也可以使用ME选项，它代表你自己的主机，和诱饵主机名混杂在一起。如果你把ME放在第六或者更靠后的位置，一些端口扫描检测软件几乎根本不会显示你的IP地址。如果你不使用ME选项，nmap会把你的IP地址随机夹杂在诱饵主机之中。

　　注意:你用来作为诱饵的主机应该正在运行或者你只是偶尔向目标发送SYN数据包。很显然，如果在网络上只有一台主机运行，目标将很轻松就会确定是哪台主机进行的扫描。或许，你还要直接使用诱饵的IP地址而不是其域名，这样诱饵网络的域名服务器的日志上就不会留下关于你的记录。

　　还要注意：一些愚蠢的端口扫描检测软件会拒绝路由试图进行端口扫描的主机。因而，你需要让目标主机和一些诱饵断开连接。如果诱饵是目标主机的网关或者就是其自己时，会给目标主机造成很大问题。所以你需要慎重使用这个选项。

　　诱饵扫描既可以在起始的ping扫描也可以在真正的扫描状态下使用。它也可以和-O选项组合使用。

　　使用太多的诱饵扫描能够减缓你的扫描速度甚至可能造成扫描结果不正确。同时，有些ISP会把你的欺骗包过滤掉。虽然现在大多数的ISP不会对此进行限制。

　　-S <IP\_Address>

　　在一些情况下，nmap可能无法确定你的源地址(nmap会告诉你)。在这种情况下，可以使用这个选项给出你的IP地址。

　　在欺骗扫描时，也使用这个选项。使用这个选项可以让目标认为是其它的主机对自己进行扫描。

　　-e

　　告诉nmap使用哪个接口发送和接受数据包。nmap能够自动对此接口进行检测，如果无效就会告诉你。

　　-g

　　设置扫描的源端口。一些天真的防火墙和包过滤器的规则集允许源端口为DNS(53)或者FTP-DATA(20)的包通过和实现连接。显然，如果攻击者把源端口修改为20或者53，就可以摧毁防火墙的防护。在使用UDP扫描时，先使用53号端口；使用TCP扫描时，先使用20号端口。注意只有在能够使用这个端口进行扫描时，nmap才会使用这个端口。例如，如果你无法进行TCP扫描，nmap会自动改变源端口，即使你使用了-g选项。

　　对于一些扫描，使用这个选项会造成性能上的微小损失，因为我有时会保存关于特定源端口的一些有用的信息。

　　-r

　　告诉nmap不要打乱被扫描端口的顺序。

　　--randomize\_hosts

　　使nmap在扫描之前，打乱每组扫描中的主机顺序，nmap每组可以扫描最多2048台主机。这样，可以使扫描更不容易被网络监视器发现，尤其和--scan\_delay 选项组合使用，更能有效避免被发现。

　　-M

　　设置进行TCP connect()扫描时，最多使用多少个套接字进行并行的扫描。使用这个选项可以降低扫描速度，避免远程目标宕机。

4.3 适时选项

　　通常，nmap在运行时，能够很好地根据网络特点进行调整。扫描时，nmap会尽量减少被目标检测到的机会，同时尽可能加快扫描速度。然而，nmap默认的适时策略有时候不太适合你的目标。使用下面这些选项，可以控制nmap的扫描timing：

-T

　　设置nmap的适时策略。Paranoid:为了避开IDS的检测使扫描速度极慢，nmap串行所有的扫描，每隔至少5分钟发送一个包； Sneaky：也差不多，只是数据包的发送间隔是15秒；Polite：不增加太大的网络负载，避免宕掉目标主机，串行每个探测，并且使每个探测有0.4 秒种的间隔；Normal:nmap默认的选项，在不是网络过载或者主机/端口丢失的情况下尽可能快速地扫描；Aggressive:设置5分钟的超时限制，使对每台主机的扫描时间不超过5分钟，并且使对每次探测回应的等待时间不超过1.5秒钟；b>Insane:只适合快速的网络或者你不在意丢失某些信息，每台主机的超时限制是75秒，对每次探测只等待0.3秒钟。你也可是使用数字来代替这些模式，例如：-T 0等于-T Paranoid，-T 5等于-T Insane。

　　这些适时模式不能下面的适时选项组合使用。

--host\_timeout

　　设置扫描一台主机的时间，以毫秒为单位。默认的情况下，没有超时限制。

--max\_rtt\_timeout

　　设置对每次探测的等待时间，以毫秒为单位。如果超过这个时间限制就重传或者超时。默认值是大约9000毫秒。

--min\_rtt\_timeout

　　当目标主机的响应很快时，nmap就缩短每次探测的超时时间。这样会提高扫描的速度，但是可能丢失某些响应时间比较长的包。使用这个选项，可以让nmap对每次探测至少等待你指定的时间，以毫秒为单位。

--initial\_rtt\_timeout

　　设置初始探测的超时值。一般这个选项只在使用-P0选项扫描有防火墙保护的主机才有用。默认值是6000毫秒。

--max\_parallelism

　　设置最大的并行扫描数量。--max\_parallelism 1表示同时只扫描一个端口。这个选项对其它的并行扫描也有效，例如ping sweep, RPC scan。

--scan\_delay

　　设置在两次探测之间，nmap必须等待的时间。这个选项主要用于降低网络的负载。

4.4 目标设定

　　在nmap的所有参数中，只有目标参数是必须给出的。其最简单的形式是在命令行直接输入一个主机名或者一个IP地址。如果你希望扫描某个IP地址的一个子网，你可以在主机名或者IP地址的后面加上/掩码。掩码在0(扫描整个网络)到32(只扫描这个主机)。使用/24扫描C类地址，/16扫描B类地址。

　　除此之外，nmap还有更加强大的表示方式让你更加灵活地指定IP地址。例如，如果要扫描这个B类网络128.210.\*.\*，你可以使用下面三种方式来指定这些地址:128.210.\*.\*、128.21-.0-255.0-255或者128.210.0.0/16这三种形式是等价的。

5.例子

　　本节将由浅入深地举例说明如何使用nmap。

nmap -v target.example.com

扫描主机target.example.com的所有TCP端口。-v打开冗余模式。

nmap -sS -O target.example.com/24

发起对target.example.com所在网络上的所有255个IP地址的秘密SYN扫描。同时还探测每台主机操作系统的指纹特征。需要root权限。

nmap -sX -p 22,53,110,143,4564 128.210.\*.1-127

对B类IP地址128.210中255个可能的8位子网的前半部分发起圣诞树扫描。确定这些系统是否打开了sshd、DNS、pop3d、imapd和4564端口。注意圣诞树扫描对Micro$oft的系统无效，因为其协议栈的TCP层有缺陷。

nmap -v --randomize\_hosts -p 80 \*.\*.2.3-5

只扫描指定的IP范围，有时用于对这个Internet进行取样分析。nmap将寻找Internet上所有后两个字节是.2.3、.2.4、.2.5的 IP地址上的WEB服务器。如果你想发现更多有意思的主机，你可以使用127-222，因为在这个范围内有意思的主机密度更大。

host -l company.com | cut -d -f 4 | ./nmap -v -iL -

列出company.com网络的所有主机，让nmap进行扫描。注意：这项命令在GNU/Linux下使用。如果在其它平台，你可能要使用 其它的命令/选项。