# nmap命令

***探测主机存活常用方式***

（1）-sP ：进行ping扫描

打印出对ping扫描做出响应的主机,不做进一步测试(如端口扫描或者操作系统探测)：

下面去扫描10.0.3.0/24这个网段的的主机

|  |  |
| --- | --- |
| 1 | nmap -sP 10.0.3.0/24 |

这个命令可以用于探测局域网有哪些机器

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11 | [root@B ~]# nmap -sP 10.0.3.0/24    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 11:24 CST  Nmap scan report for 10.0.3.1  Host is up (0.0079s latency).  Nmap scan report for 10.0.3.2  Host is up (0.0046s latency).  Nmap scan report for 10.0.3.3  Host is up (0.0037s latency).  Nmap done: 256 IP addresses (3 hosts up) scanned in 10.01 seconds  [root@B ~]# |

（2） -sn：

-sn:  Ping Scan - disable port scan  #ping探测扫描主机， 不进行端口扫描 （测试过对方主机把icmp包都丢弃掉，依然能检测到对方开机状态）

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | [root@B ~]# nmap聽 -sn 10.0.1.161-166    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 11:25 CST  Nmap scan report for 10.0.1.161  Host is up (0.00076s latency).  MAC Address: 00:0C:29:56:DE:46 (VMware)  Nmap scan report for 10.0.1.162  Host is up.  Nmap done: 6 IP addresses (2 hosts up) scanned in 0.76 seconds  [root@B ~]# |

（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）

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | [root@B ~]# nmap 10.0.1.161 -sA    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:55 CST  Nmap scan report for 10.0.1.161  Host is up (0.00030s latency).  All 1000 scanned ports on 10.0.1.161 are unfiltered  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds  [root@B ~]# nmap 10.0.1.166 -sA    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:55 CST  Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  Nmap done: 1 IP address (0 hosts up) scanned in 0.51 seconds  [root@B ~]# |

***端口扫描的高级用法***

（1） -sS ：半开放扫描（非3次握手的tcp扫描）

|  |  |
| --- | --- |
| 1  2  3  4  5 | 使用频率最高的扫描选项：SYN扫描,又称为半开放扫描，它不打开一个完全的TCP连接，执行得很快，效率高  （一个完整的tcp连接需要3次握手，而-sS选项不需要3次握手）  Tcp SYN Scan (sS) 它被称为半开放扫描  优点：Nmap发送SYN包到远程主机，但是它不会产生任何会话，目标主机几乎不会把连接记入系统日志。（防止对方判断为扫描攻击），扫描速度快，效率高，在工作中使用频率最高  缺点：它需要root/administrator权限执行 |

命令如下

|  |  |
| --- | --- |
| 1 | nmap  -sS   10.0.1.161 |

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16 | [root@B ~]# nmap  -sS   10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 11:38 CST  Nmap scan report for 10.0.1.161  Host is up (0.00028s latency).  Not shown: 995 closed ports  PORT     STATE SERVICE  22/tcp   open  ssh  111/tcp  open  rpcbind  873/tcp  open  rsync  7777/tcp open  cbt  8888/tcp open  sun-answerbook  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds  [root@B ~]# |

（2） sT：3次握手方式tcp的扫描

|  |  |
| --- | --- |
| 1  2  3  4 | Tcp connect() scan (sT)和上面的Tcp SYN 对应，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().  优点：你勿需root权限。普通用户也可以使用。  缺点：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，由于它要完成3次握手，效率低，速度慢，建议使用-sS |

nmap -sT 10.0.1.161等同于 nmap 10.0.1.161

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16 | [root@B ~]# nmap  -sT  10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 11:40 CST  Nmap scan report for 10.0.1.161  Host is up (0.00048s latency).  Not shown: 995 closed ports  PORT     STATE SERVICE  22/tcp   open  ssh  111/tcp  open  rpcbind  873/tcp  open  rsync  7777/tcp open  cbt  8888/tcp open  sun-answerbook  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds  [root@B ~]# |

（3）sU：udp端口的扫描

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.udp端口扫描速度比较慢

|  |  |
| --- | --- |
| 1 | nmap -sU 10.0.1.161 |

（4）sF：也是tcp的扫描一种，发送一个FIN标志的数据包

FIN scan(sF)

有时候TcpSYN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.

和sS扫描效果差不多，比sT速度快

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | [root@B ~]# nmap -sF  10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 11:46 CST  Nmap scan report for 10.0.1.161  Host is up (0.00050s latency).  Not shown: 997 closed ports  PORT    STATE         SERVICE  22/tcp  open|filtered ssh  111/tcp open|filtered rpcbind  873/tcp open|filtered rsync  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds  [root@B ~]# |

 -sF、-sX、-sN

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20 | 秘密FIN数据包扫描、圣诞树(XmasTree)、空(Null)扫描模式  有的防火墙可能专门阻止-sS扫描。使用这些扫描可以发送特殊标记位的数据包  比如，-sF发送一个设置了FIN标志的数据包  它们和-sS一样也需要完成TCP的握手.  和sS扫描效果差不多，都比sT速度快  除了探测报文的标志位不同，三种扫描在行为上一致  优势：能躲过一些无状态防火墙和报文过滤路由器，比SYN还要隐秘  劣势：现代的IDS产品可以发现，并非所有的系统严格遵循RFC 793      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。使用-sF、-sX、-sN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。  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。  由于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Windows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-sS（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。 |

（5）sW：窗口扫描

Window扫描，即窗口扫描

当然也可以利用Window扫描方式，得出一些端口信息，可以与之前扫描分析的结果相互补充。Window扫描方式只对某些TCPIP协议栈才有效。

它也是基于tcp的扫描，个人感觉用处不大

另外我尝试使用它对A机器的22端口扫描，发现对方22端口状态居然是错误的。

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11 | [root@B ~]# nmap -sW  10.0.1.161  -p22    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:17 CST  Nmap scan report for 10.0.1.161  Host is up (0.0027s latency).  PORT   STATE  SERVICE  22/tcp closed ssh  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds  [root@B ~]# |

（6） sV：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，如下扫描，多出了ssh的版本信息

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | [root@B ~]# nmap -sV 10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:18 CST  Nmap scan report for 10.0.1.161  Host is up (0.00017s latency).  Not shown: 997 closed ports  PORT    STATE SERVICE VERSION  22/tcp  open  ssh     OpenSSH 5.3 (protocol 2.0)  111/tcp open  rpcbind  873/tcp open  rsync   (protocol version 30)  MAC Address: 00:0C:29:56:DE:46 (VMware)    Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 6.60 seconds  [root@B ~]# |

***nmap及其少用的***

（1）iR；Choose random targets，它会随机找几个ip或者主机名进行扫描

nmap -iR 2 -Pn -p22

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | [root@B ~]# nmap -iR 2 -Pn -p22    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:51 CST  Nmap scan report for LFbn-1-4041-19.w86-233.abo.wanadoo.fr (86.233.49.19)  Host is up.  PORT   STATE    SERVICE  22/tcp filtered ssh    Nmap scan report for 209.236.30.216  Host is up.  PORT   STATE    SERVICE  22/tcp filtered ssh    Nmap done: 2 IP addresses (2 hosts up) scanned in 15.28 seconds  [root@B ~]# |

（2）--top-ports <number>: Scan <number> most common ports

#扫描常用的端口，number如果写成10，那就是扫描最常用的10个端口。比如，ssh，http，ftp等热门端口

nmap --top-ports 5 10.0.1.161

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | [root@B ~]# nmap  --top-ports 5   10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:58 CST  Nmap scan report for 10.0.1.161  Host is up (0.00074s latency).  PORT    STATE  SERVICE  21/tcp  closed ftp  22/tcp  open   ssh  23/tcp  closed telnet  80/tcp  closed http  443/tcp closed https  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds  [root@B ~]# |

（3）--port-ratio <ratio>: Scan ports more common than <ratio> #扫描常用端口里，占的比重在0.x 之上的端口

比如ratio=0.2 那么就是常用端口中占的分量超过0.2的端口，比如http的80端口

nmap --port-ratio 0.1 10.0.1.161

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16 | [root@B ~]# nmap --port-ratio 0.1 10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 13:59 CST  Nmap scan report for 10.0.1.161  Host is up (0.0011s latency).  PORT    STATE  SERVICE  21/tcp  closed ftp  22/tcp  open   ssh  23/tcp  closed telnet  25/tcp  closed smtp  80/tcp  closed http  443/tcp closed https  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds  [root@B ~]# |

（4）-sO：探测对方，TCP/IP协议簇中有哪些协议，类型号分别是多少

nmap -sO 10.0.1.161

没什么用，就是探测对方，TCP/IP协议簇中有哪些协议，类型号分别是多少

icmp即是 1 Internet控制消息

6 传输控制 协议

udp即是 17 用户数据报文

47 通用路由封装

103 协议独立多播

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20 | [root@B ~]# nmap -sO 10.0.1.161    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:00 CST  Stats: 0:04:10 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan  IPProto Scan Timing: About 91.69% done; ETC: 14:05 (0:00:23 remaining)  Nmap scan report for 10.0.1.161  Host is up (0.00082s latency).  Not shown: 249 closed protocols  PROTOCOL STATE         SERVICE  1        open          icmp  2        open|filtered igmp  6        open          tcp  17       open          udp  47       open|filtered gre  103      open|filtered pim  136      open|filtered udplite  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 289.19 seconds  [root@B ~]# |

（5）--allports

--allports (不为版本探测排除任何端口)经过我的测试，发现对于一些大的端口号，它没能检测出来 默认情况下,Nmap版本探测会跳过9100 TCP端口,因为一些打印机简单地打印送到该端口的任何数据,这回导致数十页HTTP get请求,二进制SSL会话请求等等被打印出来.这一行为可以通过修改或删除nmap-service-probes中的Exclude指示符改变,您也可以不理会任何Exclude指示符,指定--allports扫描所有端口

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | [root@A ~]# netstat   -lntp    --inet | grep -v 127.0.0.1  Active Internet connections (only servers)  Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name  tcp        0      0 0.0.0.0:45654               0.0.0.0:\*                   LISTEN      22257/nc  tcp        0      0 0.0.0.0:22                  0.0.0.0:\*                   LISTEN      2157/sshd  tcp        0      0 0.0.0.0:13306               0.0.0.0:\*                   LISTEN      21699/mysqld  tcp        0      0 0.0.0.0:873                 0.0.0.0:\*                   LISTEN      2640/rsync  tcp        0      0 0.0.0.0:111                 0.0.0.0:\*                   LISTEN      21505/rpcbind  [root@A ~]# |

如下，对于一些端口号仍然没检测出

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | [root@B ~]# nmap  10.0.1.161  --allports    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:07 CST  Nmap scan report for 10.0.1.161  Host is up (0.000098s latency).  Not shown: 997 closed ports  PORT    STATE SERVICE  22/tcp  open  ssh  111/tcp open  rpcbind  873/tcp open  rsync  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds  [root@B ~]# |

***其余很少使用的参数***

|  |  |
| --- | --- |
| 1  2  3  4 | -P0  在扫描之前，不必ping主机。有些网络的防火墙不允许ICMPecho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-PT80选项。  -PT  扫描之前，使用TCPping确定哪些主机正在运行。nmap不是通过发送ICMPecho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TCPACK包然后等待回应。 |

-A参数，综合扫描。比较慢，不推荐

-A: Enable OS detection, version detection, script scanning, and traceroute #-A综合扫描，包括系统探测，版本探测，脚本扫描，路由跟踪

nmap -A www.baidu.com

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47  48  49  50  51  52  53  54  55  56  57  58  59  60  61  62  63  64  65  66 | [root@B ~]# nmap  -A   www.baidu.com    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:10 CST  Nmap scan report for www.baidu.com (115.239.210.27)  Host is up (0.0046s latency).  Other addresses for www.baidu.com (not scanned): 115.239.211.112  Not shown: 998 filtered ports  PORT    STATE SERVICE    VERSION  80/tcp  open  http       Apache httpd  |\_http-methods: No Allow or Public header in OPTIONS response (status code 302)  | http-robots.txt: 8 disallowed entries  |\_/baidu /s? /ulink? /link? /shifen/ /homepage/ /cpro /  |\_http-title: \xE7\x99\xBE\xE5\xBA\xA6\xE4\xB8\x80\xE4\xB8\x8B\xEF\xBC\x8C\xE4\xBD\xA0\xE5\xB0\xB1\xE7\x9F\xA5\xE9\x81\x93  |\_http-favicon:  443/tcp open  ssl/https?  |\_http-title: 405 Not Allowed  |\_http-methods: No Allow or Public header in OPTIONS response (status code 405)  1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :  SF-Port443-TCP:V=5.51%T=SSL%I=7%D=12/29%Time=5864A904%P=x86\_64-redhat-linu  SF:x-gnu%r(RTSPRequest,1000,"<html>\r\n<head>\r\n<meta\x20http-equiv=\"con  SF:tent-type\"\x20content=\"text/html;charset=utf-8\">\r\n<style\x20data-f  SF:or=\"result\"\x20id=\"css\_result\">\r\nbody{color:#333;background:#fff;  SF:padding:6px\x200\x200;margin:0;position:relative;min-width:900px}body,t  SF:h,td,\.p1,\.p2{font-family:arial}p,form,ol,ul,li,dl,dt,dd,h3{margin:0;p  SF:adding:0;list-style:none}input{padding-top:0;padding-bottom:0;-moz-box-  SF:sizing:border-box;-webkit-box-sizing:border-box;box-sizing:border-box}t  SF:able,img{border:0}td{font-size:9pt;line-height:18px}\r\n\r\n\r\n\r\n#fo  SF:ot{font-size:12px}\.logo{width:117px;height:38px;cursor:pointer}\r\n\r\  SF:n#u,#head,#tool,#search,\.p1{line-height:120%;margin-left:-12pt}\.p2{wi  SF:dth:100%;line-height:120%;margin-left:-12pt}#wrapper{\_zoom:1}#container  SF:{word-break:break-all;word-wrap:break-word}\.container\_s{width:1002px}\  SF:.container\_l{width:1222px}#content\_left{width:636px;float:left;padding-  SF:left:35px}#content\_right{border-left:1px\x20solid\x20#e1e1e1;f")%r(RPCC  SF:heck,1000,"HTTP/1\.1\x20302\x20Moved\x20Temporarily\r\nServer:\x20bfe/1  SF:\.0\.8\.18\r\nDate:\x20Thu,\x2029\x20Dec\x202016\x2006:11:16\x20GMT\r\n  SF:Content-Type:\x20text/html\r\nContent-Length:\x2017931\r\nConnection:\x  SF:20close\r\nETag:\x20\"54d9748e-460b\"\r\nSet-Cookie:\x20\_\_bsi=168002475  SF:26252574989\_00\_4\_R\_N\_0\_0303\_C02F\_N\_I\_I\_0;\x20expires=Thu,\x2029-Dec-16\  SF:x2006:11:21\x20GMT;\x20domain=www\.baidu\.com;\x20path=/\r\n\r\n<html>\  SF:r\n<head>\r\n<meta\x20http-equiv=\"content-type\"\x20content=\"text/htm  SF:l;charset=utf-8\">\r\n<style\x20data-for=\"result\"\x20id=\"css\_result\  SF:">\r\nbody{color:#333;background:#fff;padding:6px\x200\x200;margin:0;po  SF:sition:relative;min-width:900px}body,th,td,\.p1,\.p2{font-family:arial}  SF:p,form,ol,ul,li,dl,dt,dd,h3{margin:0;padding:0;list-style:none}input{pa  SF:dding-top:0;padding-bottom:0;-moz-box-sizing:border-box;-webkit-box-siz  SF:ing:border-box;box-sizing:border-box}table,img{border:0}td{font-size:9p  SF:t;line-height:18px}\r\n\r\n\r\n\r\n#foot{font-size:12px}\.logo{width:11  SF:7px;height:38px;cursor:pointer}\r\n\r\n#u,#head,#tool,#");  Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  Device type: switch  Running (JUST GUESSING): HP embedded (86%)  Aggressive OS guesses: HP 4000M ProCurve switch (J4121A) (86%)  No exact OS matches for host (test conditions non-ideal).  Network Distance: 10 hops    TRACEROUTE (using port 443/tcp)  HOP RTT     ADDRESS  1   ...  2   2.75 ms 192.168.19.2  3   2.09 ms 192.168.0.1  4   ... 9  10  3.60 ms 115.239.210.27    OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  Nmap done: 1 IP address (1 host up) scanned in 30.58 seconds  [root@B ~]# |

 -e：指定网络接口,扫描时使用哪个网卡

用法 ：nmap -e eth0 targetip

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | [root@B ~]# nmap  10.0.1.161  -e eth0    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:25 CST  Nmap scan report for 10.0.1.161  Host is up (0.00020s latency).  Not shown: 997 closed ports  PORT    STATE SERVICE  22/tcp  open  ssh  111/tcp open  rpcbind  873/tcp open  rsync  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds  [root@B ~]# |

 -S：可以伪装源地址进行扫描。这样好处在于不会被对方发现自己的真实IP

[root@B ~]# nmap -e eth0 10.0.1.161 -S 10.0.1.167

WARNING: If -S is being used to fake your source address, you may also have to use -e <interface> and -Pn . If you are using it to specify your real source address, you can ignore this warning.

上面提示如果你使用-S伪装自己源地址进行扫描的话，你必须另外使用-e 指定网卡和-Pn参数才能伪装

把自己源地址伪装成10.0.1.167扫描A机器

nmap -e eth0 10.0.1.161 -S 10.0.1.167 -Pn

接下来我们来验证一下

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12 | A机器添加一条规则，比如，拒绝源地址为10.0.1.162的任何访问请求[root@A ~]# iptables -I INPUT  -s 10.0.1.162 -j DROP  [root@A ~]# iptables -L -n  Chain INPUT (policy ACCEPT)  target     prot opt source               destination  DROP       all  --  10.0.1.162           0.0.0.0/0    Chain FORWARD (policy ACCEPT)  target     prot opt source               destination    Chain OUTPUT (policy ACCEPT)  target     prot opt source               destination  [root@A ~]# |

然后我们使用B机器伪装成10.0.1.167去扫描A机器，是可以扫描成功的

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | [root@B ~]# nmap -e eth0 10.0.1.161 -S 10.0.1.167 -Pn    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:30 CST  Nmap scan report for 10.0.1.161  Host is up (0.0016s latency).  Not shown: 997 closed ports  PORT    STATE SERVICE  22/tcp  open  ssh  111/tcp open  rpcbind  873/tcp open  rsync  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds  [root@B ~]# |

假如我们在A机器上禁止源地址为10.0.1.167的访问请求，那么B机器就应该无法扫描A的端口了。我们来验证下A机器禁止源地址为10.0.1.167的机器访问

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13 | [root@A ~]# iptables -I INPUT  -s 10.0.1.167 -j DROP  [root@A ~]# iptables -L -n  Chain INPUT (policy ACCEPT)  target     prot opt source               destination  DROP       all  --  10.0.1.167           0.0.0.0/0  DROP       all  --  10.0.1.162           0.0.0.0/0    Chain FORWARD (policy ACCEPT)  target     prot opt source               destination    Chain OUTPUT (policy ACCEPT)  target     prot opt source               destination  [root@A ~]# |

B机器伪装成10.0.1.167扫描A机器，扫描不到对方端口

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | [root@B ~]# nmap -e eth0 10.0.1.161 -S 10.0.1.167 -Pn    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:33 CST  Nmap scan report for 10.0.1.161  Host is up (0.0012s latency).  All 1000 scanned ports on 10.0.1.161 are filtered  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 22.95 seconds  [root@B ~]# |

如果我们伪装成别的地址就应该能继续扫描到端口，我们伪装成了10.0.1.168，扫描成功

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | [root@B ~]# nmap -e eth0 10.0.1.161 -S 10.0.1.168 -Pn    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:34 CST  Nmap scan report for 10.0.1.161  Host is up (0.00026s latency).  Not shown: 997 closed ports  PORT    STATE SERVICE  22/tcp  open  ssh  111/tcp open  rpcbind  873/tcp open  rsync  MAC Address: 00:0C:29:56:DE:46 (VMware)    Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds  [root@B ~]# |

nmap -iflist：查看本地路由与接口

Nmap中提供了–iflist选项来查看本地主机的接口信息与路由信息。当遇到无法达到目标主机或想选择从多块网卡中某一特定网卡访问目标主机时，可以查看nmap –iflist中提供的网络接口信息。

和route  -n功能一样

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21 | [root@B ~]# nmap     -iflist    Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 14:37 CST  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INTERFACES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  DEV  (SHORT) IP/MASK       TYPE     UP MTU   MAC  lo   (lo)    127.0.0.1/8   loopback up 65536  eth0 (eth0)  10.0.1.162/24 ethernet up 1500  00:0C:29:11:64:A1    \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ROUTES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  DST/MASK       DEV  GATEWAY  10.0.1.0/24    eth0  169.254.0.0/16 eth0  0.0.0.0/0      eth0 10.0.1.1    [root@B ~]# route -n  Kernel IP routing table  Destination     Gateway         Genmask         Flags Metric Ref    Use Iface  10.0.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0  169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0  0.0.0.0         10.0.1.1        0.0.0.0         UG    0      0        0 eth0  [root@B ~]# |

nmap功能参数还有很多，个人觉得以上功能能应付工作中99%的需要了。没特殊必要，不用花太多时间在上面。

 小结：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | nmap工具很强大。建议先用Nmap扫描一个熟悉的系统，感觉一下Nmap的基本运行模式，熟悉之后，再将扫描范围扩大到其他系统。<br>首先扫描内部网络看看Nmap报告的结果，然后从一个外部IP地址扫描，注意防火墙、入侵检测系统（IDS）以及其他工具对扫描操作的反应。  通常，TCP connect()会引起IDS系统的反应（默认的nmap扫描就是sT的方式，也就是3次握手的方式扫描）  但IDS不一定会记录俗称“半连接”的TCP SYN扫描（-sS方式的）。    如果你打算熟悉和使用Nmap，下面几点经验可能对你有帮助：  1、 避免误解。不要随意选择测试Nmap的扫描目标。许多单位把端口扫描视为恶意行为，所以测试Nmap最好在内部网络进行。如有必要，应该告诉同事你正在试验端口扫描，因为扫描可能引发IDS警报以及其他网络问题。  2、 关闭不必要的服务。根据Nmap提供的报告（同时考虑网络的安全要求），关闭不必要的服务，或者调整路由器的访问控制规则（ACL），禁用网络开放给外界的某些端口。  3、 建立安全基准。在Nmap的帮助下加固网络、搞清楚哪些系统和服务可能受到攻击之后，下一步是从这些已知的系统和服务出发建立一个安全基准，以后如果要启用新的服务或者服务器，就可以方便地根据这个安全基准执行。 |

 一些nmap相关的链接，有时间可以参照下，这两篇笔记总结的比较全了

http://www.91ri.org/4105.html

http://www.91ri.org/3870.html

http://blog.163.com/jianshitianxia\_ao/blog/static/1765693842012731114821230/

https://nmap.org/download.html#windows

http://www.91ri.org/8516.html

http://blog.csdn.net/huangwwu11/article/details/20230795

http://blog.csdn.net/tan6600/article/details/45340511