nmap命令-----基础用法 - nmap - 博客园

https://www.cnblogs.com/nmap/p/6232207.html

None Fri Oct, 23 12:21

系统漏洞扫描之王-nmap

NMap，也就是Network Mapper，是Linux下的网络扫描和嗅探工具包。

其基本功能有三个:

（1）是扫描主机端口，嗅探所提供的网络服务

（2）是探测一组主机是否在线

（3）还可以推断主机所用的操作系统，到达主机经过的路由，系统已开放端口的软件版本

nmap端口状态解析 open ： 应用程序在该端口接收 TCP 连接或者 UDP 报文。 closed ：关闭的端口对于nmap也是可访问的， 它接收nmap探测报文并作出响应。但没有应用程序在其上监听。 filtered ：由于包过滤阻止探测报文到达端口，nmap无法确定该端口是否开放。过滤可能来自专业的防火墙设备，路由规则 或者主机上的软件防火墙。 unfiltered ：未被过滤状态意味着端口可访问，但是nmap无法确定它是开放还是关闭。 只有用于映射防火墙规则集的 ACK 扫描才会把端口分类到这个状态。 open | filtered ：无法确定端口是开放还是被过滤， 开放的端口不响应就是一个例子。没有响应也可能意味着报文过滤器丢弃了探测报文或者它引发的任何反应。UDP，IP协议,FIN, Null 等扫描会引起。 closed|filtered：（关闭或者被过滤的）：无法确定端口是关闭的还是被过滤的

nmap有windows和linux

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

从下面官网可以下载exe程序包和zip包

nmap常用参数

nmap扫描速度要比nc快

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：

前期准备

准备两台机器

主机A：ip地址 10.0.1.161

主机B：ip地址 10.0.1.162

B机器安装nmap的包（这个工具比较强大，习惯上每台机器都安装）

端口扫描部分

前期准备

B机器使用nmap去扫描A机器，扫描之前，A机器先查看自己上面有哪些端口在被占用

A机器上查看本地ipv4的监听端口

netstat参数解释：

-l (listen) 仅列出 Listen (监听) 的服务

-t (tcp) 仅显示tcp相关内容

-n (numeric) 直接显示ip地址以及端口，不解析为服务名或者主机名

-p (pid) 显示出socket所属的进程PID 以及进程名字

--inet 显示ipv4相关协议的监听

查看IPV4端口上的tcp的监听

netstat -lntp --inet

```
[root@A ~]# netstat   -lntp    --inet
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign
Address             State       PID/Program name
tcp        0      0 0.0.0.0:22
0.0.0.0:*                   LISTEN      2157/sshd
tcp        0      0 127.0.0.1:631
0.0.0.0:*                   LISTEN      1930/cupsd
tcp        0      0 127.0.0.1:25
0.0.0.0:*                   LISTEN      2365/master
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 ~]#
```

过滤掉监控在127.0.0.1的端口

```
[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 0.0.0.0:22
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 ~]#
```

扫描tcp端口

B机器上使用nmap扫描A机器所有端口（-p后面也可以跟空格）

下面表示扫描A机器的1到65535所有在监听的tcp端口。

nmap 10.0.1.161 -p1-65535

指定端口范围使用-p参数，如果不指定要扫描的端口，Nmap默认扫描从1到1024再加上nmap-services列出的端口

nmap-services是一个包含大约2200个著名的服务的数据库，Nmap通过查询该数据库可以报告那些端口可能对应于什么服务器，但不一定正确。

所以正确扫描一个机器开放端口的方法是上面命令。-p1-65535

注意，nmap有自己的库，存放一些已知的服务和对应端口号，假如有的服务不在nmap-services，可能nmap就不会去扫描，这就是明明一些端口已经是处于监听状态，nmap默认没扫描出来的原因，需要加入-p参数让其扫描所有端口。

虽然直接使用nmap 10.0.1.161也可以扫描出开放的端口，但是使用-p1-65535 能显示出最多的端口

区别在于不加-p 时，显示的都是已知协议的端口，对于未知协议的端口没显示

```
[root@B ~]# nmap  10.0.1.161  -p1-65535

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:11 CST
Nmap scan report for 10.0.1.161
Host is up (0.00017s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
873/tcp   open  rsync
13306/tcp open  unknown
MAC Address: 00:0C:29:56:DE:46 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
[root@B ~]#
```

如果不加-p1-65535，对于未知服务的端口（A机器的13306端口）就没法扫描到

```
[root@B ~]# nmap  10.0.1.161

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:12 CST
Nmap scan report for 10.0.1.161
Host is up (0.000089s 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 0.43 seconds
[root@B ~]#
```

扫描一个IP的多个端口

连续的端口可以使用横线连起来，端口之间可以使用逗号隔开

A机器上再启动两个tcp的监听，分别占用7777和8888端口，用于测试，加入&符号可以放入后台

```
[root@A ~]# nc -l 7777&
[1] 21779
[root@A ~]# nc -l 8888&
[2] 21780
[root@A ~]#
```

```
[root@B ~]# nmap  10.0.1.161   -p20-200,7777,8888

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:32 CST
Nmap scan report for 10.0.1.161
Host is up (0.00038s latency).
Not shown: 179 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
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 0.17 seconds
[root@B ~]#
```

扫描udp端口

先查看哪些ipv4的监听，使用grep -v排除回环接口上的监听

```
netstat -lnup --inet |grep -v 127.0.0.1
```

```
[root@A ~]# netstat -lnup --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
udp        0      0 0.0.0.0:111
0.0.0.0:*                                   21505/rpcbind
udp        0      0 0.0.0.0:631
0.0.0.0:*                                   1930/cupsd
udp        0      0 10.0.1.161:123
0.0.0.0:*                                   2261/ntpd
udp        0      0 0.0.0.0:123
0.0.0.0:*                                   2261/ntpd
udp        0      0 0.0.0.0:904
0.0.0.0:*                                   21505/rpcbind
[root@A ~]#
```

-sU：表示udp scan ， udp端口扫描

-Pn：不对目标进行ping探测（不判断主机是否在线）（直接扫描端口）

对于udp端口扫描比较慢，扫描完6万多个端口需要20分钟左右

```
[root@B ~]# nmap  -sU  10.0.1.161  -Pn

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:16 CST
Stats: 0:12:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.19% done; ETC: 10:33 (0:04:16 remaining)
Stats: 0:12:55 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.29% done; ETC: 10:33 (0:04:15 remaining)
Nmap scan report for 10.0.1.161
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE         SERVICE
111/udp open          rpcbind
123/udp open          ntp
631/udp open|filtered ipp
MAC Address: 00:0C:29:56:DE:46 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1081.27 seconds
[root@B ~]#
```

扫描多个IP用法

中间用空格分开

```
[root@B ~]# nmap 10.0.1.161  10.0.1.162

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:18 CST
Nmap scan report for 10.0.1.161
Host is up (0.000060s 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 scan report for 10.0.1.162
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.26 seconds
[root@B ~]#
```

也可以采用下面方式逗号隔开

nmap 10.0.1.161,162

```
[root@B ~]# nmap 10.0.1.161,162

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:19 CST
Nmap scan report for 10.0.1.161
Host is up (0.00025s 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 scan report for 10.0.1.162
Host is up (0.0000080s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.81 seconds
[root@B ~]#
```

扫描连续的ip地址

```
[root@B ~]# nmap 10.0.1.161-162

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:20 CST
Nmap scan report for 10.0.1.161
Host is up (0.00011s 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 scan report for 10.0.1.162
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.25 seconds
[root@B ~]#
```

扫描一个子网网段所有IP

```
[root@B ~]# nmap  10.0.3.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:21 CST
Nmap scan report for 10.0.3.1
Host is up (0.020s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
6666/tcp open  irc
8888/tcp open  sun-answerbook

Nmap scan report for 10.0.3.2
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp open     telnet

Nmap scan report for 10.0.3.3
Host is up (0.018s latency).
Not shown: 997 closed ports
PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp open     telnet

Nmap done: 256 IP addresses (3 hosts up) scanned in 14.91 seconds
[root@B ~]#
```

扫描文件里的IP

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，用法如下

```
[root@B ~]# cat ip.txt
10.0.1.161
10.0.1.162
[root@B ~]# nmap -iL ip.txt

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:23 CST
Nmap scan report for 10.0.1.161
Host is up (0.00030s 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 scan report for 10.0.1.162
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.68 seconds
[root@B ~]#
```

扫描地址段是排除某个IP地址

```
nmap 10.0.1.161-162  --exclude 10.0.1.162
```

用法如下

```
[root@B ~]# nmap 10.0.1.161-162  --exclude 10.0.1.162

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:24 CST
Nmap scan report for 10.0.1.161
Host is up (0.0022s 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 0.53 seconds
[root@B ~]#
```

扫描时排除多个IP地址

排除连续的，可以使用横线连接起来

```
nmap 10.0.1.161-163 --exclude 10.0.1.162-163
```

```
[root@B ~]# nmap 10.0.1.161-163   --exclude 10.0.1.162-163

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:25 CST
Nmap scan report for 10.0.1.161
Host is up (0.00023s 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 0.56 seconds
[root@B ~]#
```

排除分散的，使用逗号隔开

```
nmap 10.0.1.161-163 --exclude 10.0.1.161,10.0.1.163
```

```
[root@B ~]# nmap 10.0.1.161-163 --exclude 10.0.1.161,10.0.1.163

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:27 CST
Nmap scan report for 10.0.1.162
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[root@B ~]#
```

扫描多个地址时排除文件里的IP地址

（可以用来排除不连续的IP地址）

把10.0.1.161和10.0.1.163添加到一个文件里，文件名可以随意取

下面扫描10.0.1.161到10.0.1.163 这3个IP地址，排除10.0.1.161和10.0.1.163这两个IP

```
nmap 10.0.1.161-163  --excludefile ex.txt
```

```
[root@B ~]# cat ex.txt
10.0.1.161
10.0.1.163
[root@B ~]# nmap 10.0.1.161-163  --excludefile ex.txt

Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-29 10:29 CST
Nmap scan report for 10.0.1.162
Host is up (0.0000050s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@B ~]#
```