Nmap（Network Mapper）是一款安全开源的扫描工具。可以用于扫描目标网络或主机所有的开放端口，也可以探测远程主机的操作系统类型。Nmap 支持很多扫描技术，是楼主所知功能最强大的扫描工具，没有之一，虽然楼主平时仅仅用来扫描端口而已。Linux 和 Windows 都可以安装使用。

安装

```
yum install nmap -y
```

命令格式

```
nmap [扫描类型] [通用选项] [扫描目标]
```

常用参数说明

-sT #是最基本的 TCP 扫描方式。很容易被检测到，会在目标主机的日志中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)。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。

-sU #使用此选项获取某台主机上提供哪些 UDP(用户数据报协议,RFC768)服务。

-O #获得远程主机的操作系统类型。

-v #显示扫描过程中的详细信息。

-p #待扫描的端口号范围。

** 注： **

1. 详见 http://nmap.org
2. 端口取值范围是 0 - 65535(即 2 的 16 次方)，其中 0 - 1024 是系统保留

使用示例及说明

```
# nmap 127.0.0.1


Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-18 13:39 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
8088/tcp open  radan-http


Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds


# nmap -p0-65535 127.0.0.1


Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-18 13:42 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
6379/tcp  open  unknown
8088/tcp  open  radan-http
```

```
8125/tcp  open  unknown
9053/tcp  open  unknown
9056/tcp  open  unknown
19999/tcp open  unknown
21111/tcp open  unknown
39880/tcp open  unknown


Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds


# nmap -sS -O 180.00.00.xxx


Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-18 13:42 CST
Nmap scan report for 180.00.00.xxx
Host is up (0.025s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
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%)
OS CPE: cpe:/h:hp:procurve_switch_4000m
Aggressive OS guesses: HP 4000M ProCurve switch (J4121A) (86%)
No exact OS matches for host (test conditions non-ideal).
```

```
    OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

    Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds



    # nmap -sS -O -v 180.00.00.xxx



    Starting Nmap 6.40 ( http://nmap.org ) at 2017-07-18 13:49 CST

    Initiating Ping Scan at 13:49

    Scanning 180.00.00.xxx [4 ports]

    Completed Ping Scan at 13:49, 0.02s elapsed (1 total hosts)

    Initiating Parallel DNS resolution of 1 host. at 13:49

    Completed Parallel DNS resolution of 1 host. at 13:49, 0.03s elapsed

    Initiating SYN Stealth Scan at 13:49

    Scanning 180.00.00.xxx [1000 ports]

    Discovered open port 443/tcp on 180.00.00.xxx

    Discovered open port 80/tcp on 180.00.00.xxx

    Completed SYN Stealth Scan at 13:49, 4.58s elapsed (1000 total ports)

    Initiating OS detection (try #1) against 180.00.00.xxx

    Retrying OS detection (try #2) against 180.00.00.xxx

    Nmap scan report for 180.00.00.xxx

    Host is up (0.024s latency).

    Not shown: 998 filtered ports

    PORT    STATE SERVICE

    80/tcp  open  http

    443/tcp open  https
```

```
   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%)

   OS CPE: cpe:/h:hp:procurve_switch_4000m

   Aggressive OS guesses: HP 4000M ProCurve switch (J4121A) (86%)

   No exact OS matches for host (test conditions non-ideal).

   TCP Sequence Prediction: Difficulty=263 (Good luck!)

   IP ID Sequence Generation: Randomized



   Read data files from: /usr/bin/../share/nmap

   OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 9.01 seconds

             Raw packets sent: 2078 (95.116KB) | Rcvd: 23 (1.680KB)



   ** 编译安装：**
# wget http://nmap.org/dist/nmap-7.01.tar.bz2
# tar -xvf nmap-x.x.x. tar.bz2
# cd nmap-x.x.x
# ./configure --prefix=/usr/local/nmap
# make && make install
```