nmap的用法

Nmap即网络映射器对Linux系统/网络管理员来说是一个开源且非常通用的工具。Nmap用于在远程机器上探测网络，执行安全扫描，网络审计和搜寻开放端口。它会扫描远程在线主机，该主机的操作系统，包过滤器和开放的端口。

我将用两个不同的部分来涵盖大部分NMAP的使用方法，这是nmap关键的第一部分。在下面的设置中，我使用两台已关闭防火墙的服务器来测试Nmap命令的工作情况。

* 192.168.0.100 – server1.tecmint.com
* 192.168.0.101 – server2.tecmint.com

**NMAP命令用法**

# nmap [Scan Type(s)] [Options] {target specification}

**如何在Linux下安装NMAP**

现在大部分Linux的发行版本像Red Hat，CentOS，Fedoro，Debian和Ubuntu在其默认的软件包管理库（即[Yum](http://www.tecmint.com/20-linux-yum-yellowdog-updater-modified-commands-for-package-mangement/) 和 [APT](http://www.tecmint.com/useful-basic-commands-of-apt-get-and-apt-cache-for-package-management/)）中都自带了Nmap，这两种工具都用于安装和管理软件包和更新。在发行版上安装Nmap具体使用如下命令。

# yum install nmap      [on Red Hat based systems]

$ sudo apt-get install nmap [on Debian based systems]

一旦你安装了最新的nmap应用程序，你就可以按照本文中提供的示例说明来操作。

**1. 用主机名和IP地址扫描系统**

Nmap工具提供各种方法来扫描系统。在这个例子中，我使用server2.tecmint.com主机名来扫描系统找出该系统上所有开放的端口，服务和MAC地址。

**使用主机名扫描**

[root@server1 ~]# nmap server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 15:42 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.415 seconds

You have new mail in /var/spool/mail/root

**使用IP地址扫描**

[root@server1 ~]# nmap 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-18 11:04 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

958/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.465 seconds

You have new mail in /var/spool/mail/root

**2.扫描使用“-v”选项**

你可以看到下面的命令使用“ **-v**“选项后给出了远程机器更详细的信息。

[root@server1 ~]# nmap -v server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 15:43 EST

Initiating ARP Ping Scan against 192.168.0.101 [1 port] at 15:43

The ARP Ping Scan took 0.01s to scan 1 total hosts.

Initiating SYN Stealth Scan against server2.tecmint.com (192.168.0.101) [1680 ports] at 15:43

Discovered open port 22/tcp on 192.168.0.101

Discovered open port 80/tcp on 192.168.0.101

Discovered open port 8888/tcp on 192.168.0.101

Discovered open port 111/tcp on 192.168.0.101

Discovered open port 3306/tcp on 192.168.0.101

Discovered open port 957/tcp on 192.168.0.101

The SYN Stealth Scan took 0.30s to scan 1680 total ports.

Host server2.tecmint.com (192.168.0.101) appears to be up ... good.

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.485 seconds

               Raw packets sent: 1681 (73.962KB) | Rcvd: 1681 (77.322KB)

**3.扫描多台主机**

你可以简单的在Nmap命令后加上多个IP地址或主机名来扫描多台主机。

[root@server1 ~]# nmap 192.168.0.101 192.168.0.102 192.168.0.103

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:06 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 3 IP addresses (1 host up) scanned in 0.580 seconds

**4.扫描整个子网**

你可以使用\*通配符来扫描整个子网或某个范围的IP地址。

[root@server1 ~]# nmap 192.168.0.\*

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:11 EST

Interesting ports on server1.tecmint.com (192.168.0.100):

Not shown: 1677 closed ports

PORT    STATE SERVICE

22/tcp  open  ssh

111/tcp open  rpcbind

851/tcp open  unknown

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 256 IP addresses (2 hosts up) scanned in 5.550 seconds

You have new mail in /var/spool/mail/root

从上面的输出可以看到，nmap扫描了整个子网，给出了网络中当前网络中在线主机的信息。

**5.使用IP地址的最后一个字节扫描多台服务器**

你可以简单的指定IP地址的最后一个字节来对多个IP地址进行扫描。例如，我在下面执行中扫描了IP地址192.168.0.101，192.168.0.102和192.168.0.103。

[root@server1 ~]# nmap 192.168.0.101,102,103

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:09 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 3 IP addresses (1 host up) scanned in 0.552 seconds

You have new mail in /var/spool/mail/root

**6. 从一个文件中扫描主机列表**

如果你有多台主机需要扫描且所有主机信息都写在一个文件中，那么你可以直接让nmap读取该文件来执行扫描，让我们来看看如何做到这一点。

创建一个名为“nmaptest.txt ”的文本文件，并定义所有你想要扫描的服务器IP地址或主机名。

[root@server1 ~]# cat > nmaptest.txt

localhost

server2.tecmint.com

192.168.0.101

接下来运行带“**iL”** 选项的nmap命令来扫描文件中列出的所有IP地址

[root@server1 ~]# nmap -iL nmaptest.txt

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-18 10:58 EST

Interesting ports on localhost.localdomain (127.0.0.1):

Not shown: 1675 closed ports

PORT    STATE SERVICE

22/tcp  open  ssh

25/tcp  open  smtp

111/tcp open  rpcbind

631/tcp open  ipp

857/tcp open  unknown

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

958/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

958/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 3 IP addresses (3 hosts up) scanned in 2.047 seconds

**7.扫描一个IP地址范围**

你可以在nmap执行扫描时指定IP范围。

[root@server1 ~]# nmap 192.168.0.101-110

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:09 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 10 IP addresses (1 host up) scanned in 0.542 seconds

**8.排除一些远程主机后再扫描**

在执行全网扫描或用通配符扫描时你可以使用“-**exclude**”选项来排除某些你不想要扫描的主机。

[root@server1 ~]# nmap 192.168.0.\* --exclude 192.168.0.100

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:16 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 255 IP addresses (1 host up) scanned in 5.313 seconds

You have new mail in /var/spool/mail/root

**9.扫描操作系统信息和路由跟踪**

使用Nmap，你可以检测远程主机上运行的操作系统和版本。为了启用操作系统和版本检测，脚本扫描和路由跟踪功能，我们可以使用NMAP的“**-A**“选项。

[root@server1 ~]# nmap -A 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:25 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 4.3 (protocol 2.0)

80/tcp   open  http    Apache httpd 2.2.3 ((CentOS))

111/tcp  open  rpcbind  2 (rpc #100000)

957/tcp  open  status   1 (rpc #100024)

3306/tcp open  mysql   MySQL (unauthorized)

8888/tcp open  http    lighttpd 1.4.32

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).

TCP/IP fingerprint:

SInfo(V=4.11%P=i686-redhat-linux-gnu%D=11/11%Tm=52814B66%O=22%C=1%M=080027)

TSeq(Class=TR%IPID=Z%TS=1000HZ)

T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T2(Resp=N)

T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Uptime 0.169 days (since Mon Nov 11 12:22:15 2013)

Nmap finished: 1 IP address (1 host up) scanned in 22.271 seconds

从上面的输出你可以看到，Nmap显示出了远程主机**操作系统的TCP** / **IP**协议指纹，并且更加具体的显示出远程主机上的端口和服务。

**10.启用Nmap的操作系统探测功能**

使用选项“**-O**”和“**-osscan-guess**”也帮助探测操作系统信息。

[root@server1 ~]# nmap -O server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:40 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).

TCP/IP fingerprint:

SInfo(V=4.11%P=i686-redhat-linux-gnu%D=11/11%Tm=52815CF4%O=22%C=1%M=080027)

TSeq(Class=TR%IPID=Z%TS=1000HZ)

T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T2(Resp=N)

T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=Option -O and -osscan-guess also helps to discover OS

R%Ops=)

T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Uptime 0.221 days (since Mon Nov 11 12:22:16 2013)

Nmap finished: 1 IP address (1 host up) scanned in 11.064 seconds

You have new mail in /var/spool/mail/root

**11.扫描主机侦测防火墙**

下面的命令将扫描远程主机以探测该主机是否使用了包过滤器或防火墙。

[root@server1 ~]# nmap -sA 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:27 EST

All 1680 scanned ports on server2.tecmint.com (192.168.0.101) are UNfiltered

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.382 seconds

You have new mail in /var/spool/mail/root

**12.扫描主机检测是否有防火墙保护**

扫描主机检测其是否受到数据包过滤软件或防火墙的保护。

[root@server1 ~]# nmap -PN 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:30 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.399 seconds

**13.找出网络中的在线主机**

使用“**-sP**”选项，我们可以简单的检测网络中有哪些在线主机，该选项会跳过端口扫描和其他一些检测。

[root@server1 ~]# nmap -sP 192.168.0.\*

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-18 11:01 EST

Host server1.tecmint.com (192.168.0.100) appears to be up.

Host server2.tecmint.com (192.168.0.101) appears to be up.

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 256 IP addresses (2 hosts up) scanned in 5.109 seconds

**14.执行快速扫描**

你可以使用“**-F**”选项执行一次快速扫描，仅扫描列在nmap-services文件中的端口而避开所有其它的端口。

[root@server1 ~]# nmap -F 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:47 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1234 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.322 seconds

**15.查看Nmap的版本**

你可以使用“**-V**”选项来检测你机子上Nmap的版本。

[root@server1 ~]# nmap -V

Nmap version 4.11 ( http://www.insecure.org/nmap/ )

You have new mail in /var/spool/mail/root

**16.顺序扫描端口**

使用“**-r**”选项表示不会随机的选择端口扫描。

[root@server1 ~]# nmap -r 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 16:52 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.363 seconds

**17.打印主机接口和路由**

你可以使用nmap的“**–iflist**”选项检测主机接口和路由信息。

[root@server1 ~]# nmap --iflist

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:07 EST

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INTERFACES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

DEV  (SHORT) IP/MASK          TYPE     UP MAC

lo   (lo)    127.0.0.1/8      loopback up

eth0 (eth0)  192.168.0.100/24 ethernet up 08:00:27:11:C7:89

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ROUTES\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

DST/MASK      DEV  GATEWAY

192.168.0.0/0 eth0

169.254.0.0/0 eth0

从上面的输出你可以看到，nmap列举出了你系统上的接口以及它们各自的路由信息。

**18.扫描特定的端口**

使用Nmap扫描远程机器的端口有各种选项，你可以使用“-**P**”选项指定你想要扫描的端口，默认情况下nmap只扫描**TCP**端口。

[root@server1 ~]# nmap -p 80 server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:12 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT   STATE SERVICE

80/tcp open  http

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) sca

**19.扫描TCP端口**

你可以指定具体的端口类型和端口号来让nmap扫描。

[root@server1 ~]# nmap -p T:8888,80 server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:15 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT     STATE SERVICE

80/tcp   open  http

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.157 seconds

**20.扫描UDP端口**

[root@server1 ~]# nmap -sU 53 server2.tecmint.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:15 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT     STATE SERVICE

53/udp   open  http

8888/udp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.157 seconds

**21.扫描多个端口**

你还可以使用选项“-**P**”来扫描多个端口。

[root@server1 ~]# nmap -p 80,443 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-18 10:56 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT    STATE  SERVICE

80/tcp  open   http

443/tcp closed https

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.190 seconds

**22.扫描指定范围内的端口**

您可以使用表达式来扫描某个范围内的端口。

[root@server1 ~]#  nmap -p 80-160 192.168.0.101

**23.查找主机服务版本号**

[root@server1 ~]# nmap -sV 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:48 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 4.3 (protocol 2.0)

80/tcp   open  http    Apache httpd 2.2.3 ((CentOS))

111/tcp  open  rpcbind  2 (rpc #100000)

957/tcp  open  status   1 (rpc #100024)

3306/tcp open  mysql   MySQL (unauthorized)

8888/tcp open  http    lighttpd 1.4.32

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 12.624 seconds

**24.使用TCP ACK (PA)和TCP Syn (PS)扫描远程主机**

有时候包过滤防火墙会阻断标准**的ICMP**ping请求，在这种情况下，我们可以使用**TCP ACK**和**TCP Syn**方法来扫描远程主机。

[root@server1 ~]# nmap -PS 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 17:51 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.360 seconds

You have new mail in /var/spool/mail/root

**25.使用TCP ACK扫描远程主机上特定的端口**

[root@server1 ~]# nmap -PA -p 22,80 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 18:02 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT   STATE SERVICE

22/tcp open  ssh

80/tcp open  http

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.166 seconds

You have new mail in /var/spool/mail/root

**26. 使用TCP Syn扫描远程主机上特定的端口**

[root@server1 ~]# nmap -PS -p 22,80 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 18:08 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

PORT   STATE SERVICE

22/tcp open  ssh

80/tcp open  http

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.165 seconds

You have new mail in /var/spool/mail/root

**27.执行一次隐蔽的扫描**

[root@server1 ~]# nmap -sS 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 18:10 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.383 seconds

You have new mail in /var/spool/mail/root

**28.使用TCP Syn扫描最常用的端口**

[root@server1 ~]# nmap -sT 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 18:12 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

80/tcp   open  http

111/tcp  open  rpcbind

957/tcp  open  unknown

3306/tcp open  mysql

8888/tcp open  sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 0.406 seconds

You have new mail in /var/spool/mail/root

**29.执行TCP空扫描以骗过防火墙**

[root@server1 ~]# nmap -sN 192.168.0.101

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-11 19:01 EST

Interesting ports on server2.tecmint.com (192.168.0.101):

Not shown: 1674 closed ports

PORT     STATE         SERVICE

22/tcp   open|filtered ssh

80/tcp   open|filtered http

111/tcp  open|filtered rpcbind

957/tcp  open|filtered unknown

3306/tcp open|filtered mysql

8888/tcp open|filtered sun-answerbook

MAC Address: 08:00:27:D9:8E:D7 (Cadmus Computer Systems)

Nmap finished: 1 IP address (1 host up) scanned in 1.584 seconds

You have new mail in /var/spool/mail/root