Getting ready

Various commands are available for listing ports and services running on each port (for example, `lsof` and `netstat`). These commands are, by default, available on all GNU/Linux distributions.

How to do it...

In order to list all opened ports on the system along with the details on each service attached to it, use:

```
$ lsof -i
COMMAND    PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
firefox-b 2261 slynux   78u  IPv4  63729      0t0  TCP localhost:47797->localhost:42486 (ESTABLISHED)
firefox-b 2261 slynux   80u  IPv4  68270      0t0  TCP slynux-laptop.local:41204->192.168.0.2:3128 (CLOSE_WAIT)
firefox-b 2261 slynux   82u  IPv4  68195      0t0  TCP slynux-laptop.local:41197->192.168.0.2:3128 (ESTABLISHED)
ssh       3570 slynux    3u  IPv6  30025      0t0  TCP localhost:39263->localhost:ssh (ESTABLISHED)
ssh       3836 slynux    3u  IPv4  43431      0t0  TCP slynux-laptop.local:40414->boneym.mtveurope.org:422 (ESTABLISHED)
GoogleTal 4022 slynux   12u  IPv4  55370      0t0  TCP localhost:42486 (LISTEN)
GoogleTal 4022 slynux   13u  IPv4  55379      0t0  TCP localhost:42486->localhost:32955 (ESTABLISHED)
```

Each entry in the output of `lsof` corresponds to each service that opens a port for communication. The last column of output consists of lines similar to:

```
laptop.local:41197->192.168.0.2:3128
```

In this output, `laptop.local:41197` corresponds to the localhost and `192.168.0.2:3128` corresponds to the remote host. `41197` is the port opened from the current machine, and `3128` is the port to which the service connects at the remote host.

In order to list out the opened ports from the current machine, use:

```
$ lsof -i | grep ":[0-9]\+->" -o | grep "[0-9]\+" -o  | sort | uniq
```

How it works...

The `:[0-9]\+->` regex for `grep` is used to extract the host port portion (`:34395->`) from the `lsof` output. The next `grep` is used to extract the port number (which is numeric). Multiple connections may occur through the same port and hence, multiple entries of the same port may occur. In order to display each port once, they are sorted and the unique ones are printed.

There's more...

Let's go through additional utilities that can be used for viewing the opened port and network traffic related information.

Opened port and services using netstat

`netstat` is another command for the network service analysis. Explaining all the features of `netstat` is not in the scope of this recipe. We will now look at how to list services and port numbers.

Use `netstat -tnp` to list opened port and services as follows:

```
$ netstat -tnp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 192.168.0.82:38163      192.168.0.2:3128
ESTABLISHED 2261/firefox-bin
tcp        0      0 192.168.0.82:38164      192.168.0.2:3128        TIME_
WAIT   -
tcp        0      0 192.168.0.82:40414      193.107.206.24:422
ESTABLISHED 3836/ssh
tcp        0      0 127.0.0.1:42486         127.0.0.1:32955
ESTABLISHED 4022/GoogleTalkPlug
tcp        0      0 192.168.0.82:38152      192.168.0.2:3128
ESTABLISHED 2261/firefox-bin
tcp6       0      0 ::1:22                  ::1:39263
ESTABLISHED -
tcp6       0      0 ::1:39263               ::1:22
ESTABLISHED 3570/ssh
```