ADANAC SOFTWARE

Some common Unix network ports on my server and what they mean

By Dirk Hart

One of the rules of thumb for system security is to turn off the ports you don't need. It had never really concerned me, as my Unix box is behind a router and the router doesn't forward any ports except for a couple I have specifically allowed.

I was a bit surprised the other day when I scanned ports 1-1024 on my SCO Unix box and found ports 1, 7, 9, 13, 19, 21, 23, 25, 37, 79, 110, 137, 139, 199, 210, 457, 512, 513, 514, 515, were all alive. I could identify some of these, and heard about others and knew generically what they were but some were a complete mystery.

By convention, there are 3 types or ranges of port numbers. There are the Well Known Ports, the Registered Ports, and the Private Ports.

The Well Known Ports run from 0 through 1023, the Registered Ports range from 1024 through 49151, and the Private Ports go from 49152 through 65535. For a big list of ports, browse to http://www.iana.org/assignments/port-numbers. We're just going to talk about some of the well known ports here.

Tcpmux is a service that runs on port 1. According to RFC 1078 it is supposed to accept a request for a service listed in inetd.conf and hook you up. I used telnet (telnet 192.168.1.1 1) to try this on my SCO Unix 504 box and that's not what happened. I thought that maybe I typed in the name of the service incorrectly, so I typed in help, which according to RFC1078 is a required feature of tcpmux. No cigar. I edited /etc/inetd.conf and commented out the line with tcpmux, restarted inetd, and was still able to telnet to my SCO box. I concluded that tcpmux is not required on SCO 504, so I left it turned off.

Port 7 is for echo. Using telnet (telnet 192.168.1.1 7) I connected to echo, and as you might expect everything I typed was displayed. Echo has been described as useful for debugging, but I've never used it. I turned off echo by commenting out that line in /etc/inetd.conf and restarted inetd.

To restart inetd I typed in ps -ef|grep inetd and noted the process ID (PID) in the second column. Then I typed kill -1 <PID>. This causes inetd to reread inetd.conf. It won't say anything as all the job is done silently.

Port 9 is for a service called discard. I telneted to port 9, typed stuff in, saw it displayed back to me. This was not what I expected, since discard is supposed to discard all the tcp and udp packets sent to it. In any case, I found discard to be even more droll than echo. It got the usual treatment.

Port 11 is meant for systat. This sounded like fun, but when I tried telnet 192.168.1.1 11 all I got was:

```
Trying 192.168.1.1...
telnet: Unable to connect to remote host: Connection refused
```

Since it didn't seem to work I looked in /etc/services where it was indeed listed. Next, I looked in /etc/inetd.conf where there was some interesting stuff, but nothing called systat.

The word systat suggests system statistics to me and that's exciting stuff for computer nerds, so I edited inetd.conf and following some of the examples already there, I added this at the end:

```
#### bold experiment
systat  stream  tcp     nowait  root    /bin/who
```

Intrepidly I entered telnet 192.168.1.1 11 and was greeted with:

```
    dhart      ttyp0        Aug 27 17:56
```

But I digress, and who isn't that interesting after all, so I deleted my bold experiment from inetd.conf and restarted inetd.

Port 13 was more fun than the other ports. I typed in telnet 192.168.1.1 13 and was greeted with:

```
Trying 192.168.1.1...
Connected to bali.
Escape character is '^]'.
Wed Aug 27 18:17:40 2003
Connection closed by foreign host.
```

Other than noting it was time for dinner this was a bit of a snore so I turned that off too.

Port 19 was quite annoying - I typed in telnet 192.168.1.1 19 and saw a sliding pattern of characters. This must be a holdover from tty and dumb terminal days but I have never used chargen and I'm not going to start now. I don't even know how you would use a dumb terminal to access this service. Chargen jangled my nerves and I turned it off.

Port 21 is well known for providing FTP services. I telnet to port 21 and got an FTP login. Now FTP can be quite useful, but it's also known as a gaping security hole. Since my router is not currently allowing incoming FTP I left this service turned on. If your Unix machine is on the internet you should seriously consider turning this off.

Port 23 is the telnet port. Since my LAN is secure I've left it turned on. It's really quite useful, but certainly a large security concern if folks can gain access to your Unix box from the internet. Use your router to restrict access to a few known IP addresses, or use SSH or a VPN.

Port 25 is one of my favourites. This is the port used by SMTP which is the most commonly used protocol used to transfer email these days. I telneted to a well known site:

```
# telnet pcunix.com 25
Trying 64.226.42.29...
Connected to pcunix.com.
Escape character is '^]'.
220 vps.pcunix.com ESMTP Sendmail 8.11.6/8.11.0; Wed, 27 Aug 2003 22:48:05 GMT
helo greatwall.linux.com
250 vps.pcunix.com Hello h000800504e8d.ne.client2.attbi.com [65.96.73.149], pleased to meet you
```

How nice to be so cordially greeted! Well, there's no email without port 25, and Tony doesn't let me play with his computer, so we're leaving that one as we found it.

Port 37 support then time daemon. It is supposed to synchronize your Unix box's time with the time of other boxes running timed. This can be quite handy, but can give unpredictable results if not properly implemented. Time has run out for this service.

The finger daemon runs on port 79. You can use finger to get information about user accounts, but it also provides spammers and hackers with user names and accounts. Again, I used telnet to connect to port 79 and typed in a user name:

```
# telnet cuba 79
Trying 192.168.1.1...
Connected to cuba.
Escape character is '^]'.
teddy
Login: teddy                    Name: Teddy Roosevelt
Directory: /usr/teddy           Shell: /bin/ksh
On since Wed Aug 27 17:56 on ttyp0 (messages off) from sanjuanhill
No unread mail
Project:
Panama Canal.
Plan:
A man a plan a canal Panama
Connection closed by foreign host.
```

This one gets turned off too. No one uses it anymore anyways.

Port 110 is interesting. It gives us the POP daemon that lets us get mail (not to be confused with say, IMAP). Using our trusty telnet we connect to the SCO box on port 110:

```
# telnet bali 110
Trying 192.168.1.1...
Connected to bali.
Escape character is '^]'.
+OK POP3 server on bali started on Wed Aug 27 22:59:02 2003          USER BOOPY
```

```
+OK Password required for BOOPY
pass topsecret
+OK BOOPY's maildrop has 0  messages (0 octets)       quit
Connection closed by foreign host.
```

Presto! we are ready to get mail. A list of commands is available in RFC 1939. I leave this one enabled, but if you don't get mail off your unix box you might try disabling it.

Ports 137, 138 and 139 all have to do with NETBIOS. NETBIOS is the Windows protocol responsible for chit-chat between Windows machines. Windows machine exchange names, shares, data and such using NETBIOS. These ports are used by daemons providing Windows style networking (SMB or CIFS) such as Samba or FacetWin. These packages let your Windows machines see disk and printer shares configured on your Unix machine without having to add any software to Windows. Port 137 is NETBIOS name resolution, 138 is for NETBIOS data, and 139 is for NETBIOS session protocol.

If you have a LAN with Windows machines you MUST have a router configured to block port 137. There are two reasons that come to mind right away.

First, because NETBIOS is not routable M$ has implemented NETBIOS over TCP/IP, making it routable. This put YOUR name resolution packets out on the internet. DOH! How many people have a PC at home with cable or DSL that don't know this? I'm quite sure the folks selling software firewalls don't want you to know that you can disable NETBIOS over TCP/IP too. Yet another entire industry created by M$ to marry it's first cousin, the anti-virus industry. But I digress.

Second, some viruses such as Nimda, use port 137 to discover shares. Again, if your PC is directly on the internet with out the protection of a router, you are not part of the solution.

If you have no need for sharing your unix machines disk or printers make sure these services are turned off.

Port 199. The most mysterious port so far. Network View showed this port to be active. I looked in services and saw that smux runs on port 199 but when I checked inetd.conf, it was not listed. A quick trip to google.com revealed that smux uses port 199 and sure enough, when I typed ps -ef|grep snmpd, there it was. smux is part of SNMP (Simple Network Management Protocol). It is described in RFC 1227. One day I may use SNMP, but not today. On SCO Unix you can disable snmpd by renamed /etc/snmpd.conf or by commenting the appropriate lines in /etc/rc2.d/S85tcp.

Port 210 was not even listed in /etc/services nor in /etc/inetd.conf. Only by using a tool like Network View would you know that it was open. This port is used by WAIS (Wide Area Information System) and is used to distribute information in one or more databases. It is running on my SCO box to support SCO's technical information CDROMS. These haven't been updated in a long time but since this information is rumoured to be taken down off the web as well I'll keep wais running.

Port 457 runs httpd in support of WAIS and the SCO technical information CDROM. It stays for now.

```
# telnet bali 457
Trying 192.168.1.1...
Connected to bali.
Escape character is '^]'.
http
<HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY><H1>400 Bad Request</H1>
Your client sent a query that this server could not
understand.<P>
Reason: Invalid or unsupported method.<P>
</BODY>
Connection closed by foreign host.
```

As you can see I typed http after connecting and httpd informs me I do not speak the lingua franca. Merde.

Port 512 is interesting as it has different services on the same port. Exec responds to tcp while biff responds to udp. Note that exec refers to a line in inetd.conf that starts the rexecd daemon.

```
exec          512/tcp
biff          512/udp        comsat
```

Rexecd lets you execute programs on a host running rexecd. Authentication is based on user names and passwords. This sounds way kewl but I've never had cause to do this so I turned that off.

Biff is interesting as well. It lets the system know that you want to be notified when new mail arrives for you. As root I sent mail to a well known user:

```
# mail dhart
Subject: raven

Once upon a midnight dreary,
as I sat weak and weary.
poring over some half forgotten tomes of lore
EOT
#
```

and presently on the session where dhart was logged in this appeared:

```
$

New mail for dhart@bali.adanac has arrived:
----
From: root@bali.adanac.com (Superuser)
Subject: raven
test
```

Well, I don't know about you, but I don't read my mail on the Unix box - I pop it to my PC and use the Mozilla MUA. I think we can do without this service.

Port 513 is used by two services as well. rlogin runs on tcp and who runs on udp. On my SCO box who wasn't configured, but it is used to send regular broadcasts of who is logged in, and individual machines make a database of who is logged in and on which machine.

Rlogin lets users connect from remote machines that are listed in .rhosts. It is apparently more capable than telnet but I've never used it. There are a number of rlogin exploits, so this gets the axe as well.

Port 514 is used by both cmd and syslog.

Cmd points to a line in inetd.conf that runs the rshd. Rshd provides rcmd for users listed in hosts.equiv. There are versions that use Kerberos authentication that listen on port 544, but this SCO box have that stuff. I once used rcmd/rcp on a HPUX machine and it was very cool. I don't use it here though, so that can go.

Syslog basically collects comments from several sources and puts them in a file. These comments are real handy when you're trying to figure out what went wrong with your stuff. One of the places syslog gets stuff is from port 514 - not only can you log your own stuff, but you can log other hosts stuff too. Unfortunately, there are syslog exploits too, so as I wasn't using it, I turned it off.

Port 515 supports the spooler. Again, this is a mystery port as it is not mentioned in inetd.conf. Nor are the words printer nor spooler in inetd.conf. And if you try ps -ef|grep printer (or spooler) you will be met with disappointment. Fortunately most nerds know that you have to look for lp. I did:

```
root   316     1  0   Jul-21       ?    00:00:00 /usr/lib/lpd
```

Not only does lpd let you spool up and subsequently print stuff, but when properly configured it will let you print stuff to a printer attached to another host. This is wicked kewl, but I have only one SCO box. Kewl as it is, I turned it off.

Thats all the well known ports on my SCO box. Most of the services were unused and I'd bet that most of the services on your SCO box are unused as well.