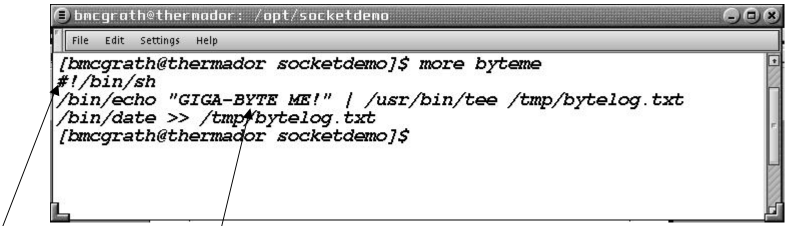
socket demo

What are we doing

- creating a simple shell script to be run
- add service to /etc/services
- add script to /etc/xinetd.d for the service
- restart xinetd to start
- test with telnet
- use ntsysv to start and stop
- check and see what ntsysv is doing

Create a script

This is what will run when we access out service



```
[bmcgrath@thermador socketdemo]$ more byteme
#!/bin/sh
/bin/echo "GIGA-BYTE ME!" | /usr/bin/tee /tmp/bytelog.txt
/bin/date >> /tmp/bytelog.txt
[bmcgrath@thermador socketdemo]$
```

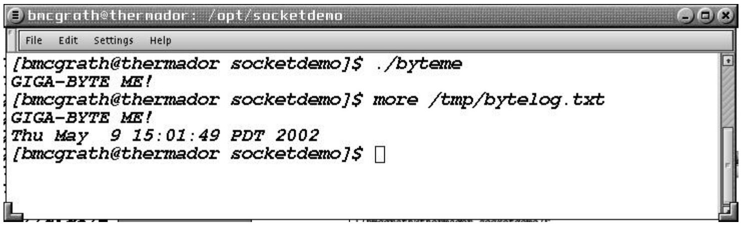
Start a shell

Cheerful networking message tee'd to a log file which has the date and time appended to it

Test it from the command line

Sends message to stdout

Sends message and timestamp to log file



```
[bmcgrath@thermador socketdemo]$ ./byteme
GIGA-BYTE ME!
[bmcgrath@thermador socketdemo]$ more /tmp/bytelog.txt
GIGA-BYTE ME!
Thu May  9 15:01:49 PDT 2002
[bmcgrath@thermador socketdemo]$ 
```

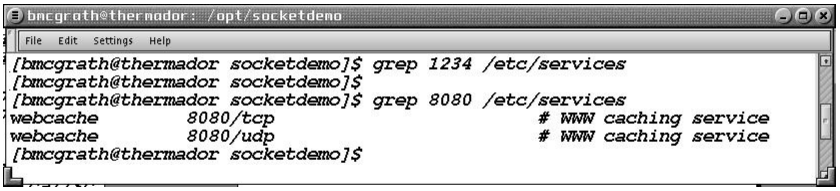
Make sure you are not at root (you should be able to run the service as anybody)

Pick a name and number

Sockets with numbers less than 1024 are root

When you pick a number grep against /etc/services to make sure it's not already used.

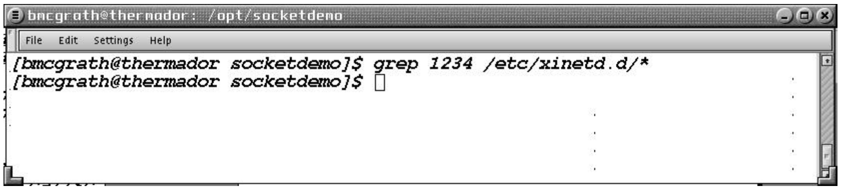
We'll try 1234



```
[bmcgrath@thermador socketdemo]$ grep 1234 /etc/services
[bmcgrath@thermador socketdemo]$
[bmcgrath@thermador socketdemo]$ grep 8080 /etc/services
webcache        8080/tcp                        # WWW caching service
webcache        8080/udp                        # WWW caching service
[bmcgrath@thermador socketdemo]$
```

1234 is not used - 8080 is

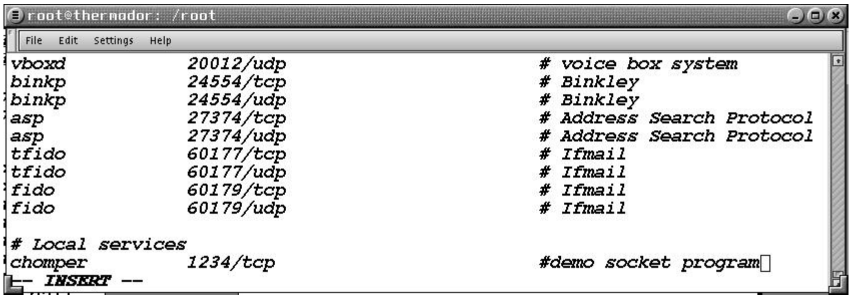
Check for references in xinetd.d



```
[bmcgrath@thermador socketdemo]$ grep 1234 /etc/xinetd.d/*
[bmcgrath@thermador socketdemo]$ 
```

In case there's a script in xinetd.d calling a service not in /etc/services

Select an improbable name and add a new entry in /etc/services

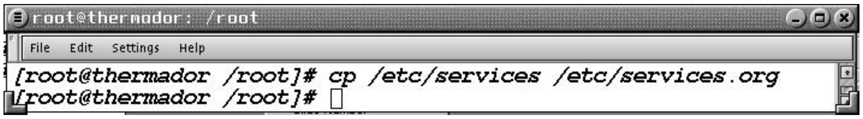


```
vboxd           20012/udp                       # voice box system
binkp           24554/tcp                       # Binkley
binkp           24554/udp                       # Binkley
asp             27374/tcp                       # Address Search Protocol
asp             27374/udp                       # Address Search Protocol
tfido           60177/tcp                       # Ifmail
tfido           60177/udp                       # Ifmail
fido            60179/tcp                       # Ifmail
fido            60179/udp                       # Ifmail

# Local services
chomper         1234/tcp                        #demo socket program
-- INSERT --
```

After the # Local Services header at the end

YOU DIDN'T FORGET DID YOU????

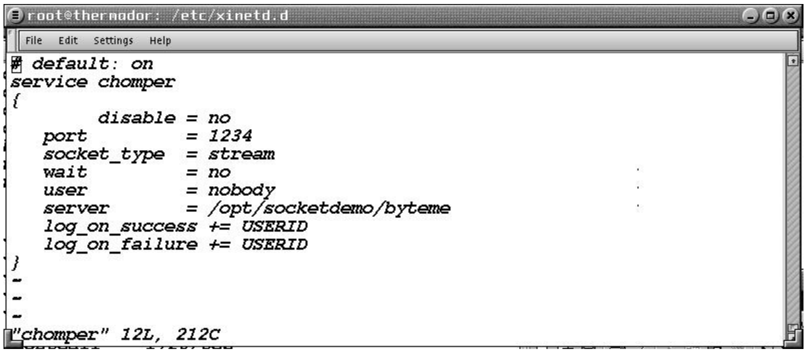


```
[root@thermador /root]# cp /etc/services /etc/services.org
[root@thermador /root]#
```

WELL - DID YOU????

If you don't save these config files - you are going to hell in a sled and nobody is going to feel sorry for you!!!!!

create a chomper script in /etc/xinetd.d



```
# default: on
service chomper
{
        disable = no
   port         = 1234
   socket_type  = stream
   wait         = no
   user         = nobody
   server       = /opt/socketdemo/byteme
   log_on_success += USERID
   log_on_failure += USERID
}
~
~
~
"chomper" 12L, 212C
```

The fields

disable - determines state when xinetd starts

port - number associated with service

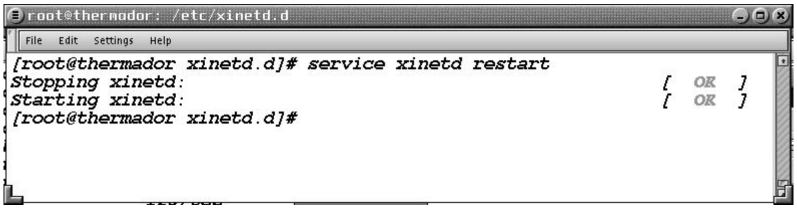
socket_type - streams (tcp) or dgram (udp) mostly

server - the program you want to run ABSOLUTE PATH!

user - entry must by in /etc/passwd (nobody = everybody)

wait - yes = single thread / no = multithread

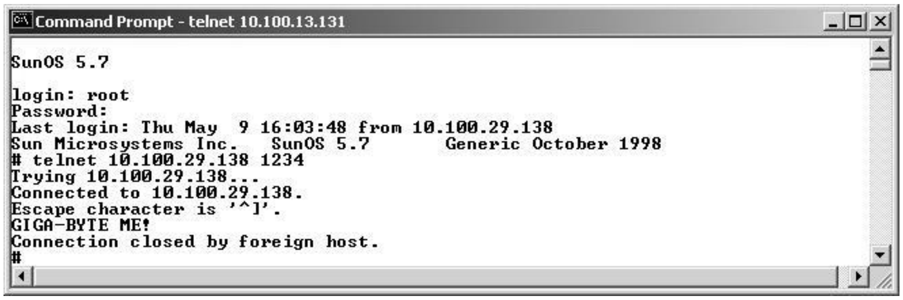
restart xinetd



```
[root@thermador xinetd.d]# service xinetd restart
Stopping xinetd:                                          [  OK  ]
Starting xinetd:                                          [  OK  ]
[root@thermador xinetd.d]#
```

try it from another station

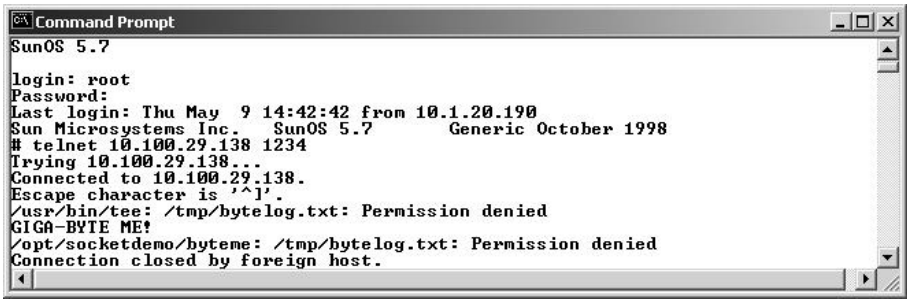
telnet <ip address> 1234



```
SunOS 5.7

login: root
Password:
Last login: Thu May  9 16:03:48 from 10.100.29.138
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
# telnet 10.100.29.138 1234
Trying 10.100.29.138...
Connected to 10.100.29.138.
Escape character is '^]'.
GIGA-BYTE ME!
Connection closed by foreign host.
#
```

If you have a problem...

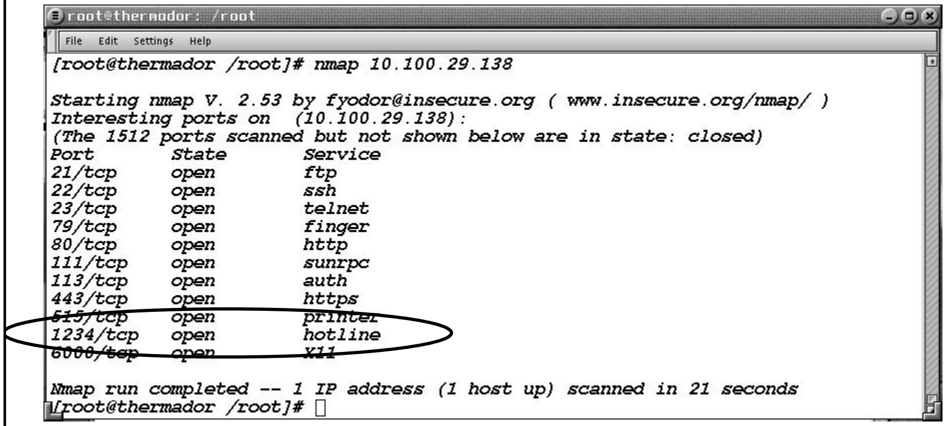


```
SunOS 5.7

login: root
Password:
Last login: Thu May  9 14:42:42 from 10.1.20.190
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
# telnet 10.100.29.138 1234
Trying 10.100.29.138...
Connected to 10.100.29.138.
Escape character is '^]'.
/usr/bin/tee: /tmp/bytelog.txt: Permission denied
GIGA-BYTE ME!
/opt/socketdemo/byteme: /tmp/bytelog.txt: Permission denied
Connection closed by foreign host.
```

You tested the program on your station with wrong permissions for nobody. You don't have permission to overwrite the file

port 1234



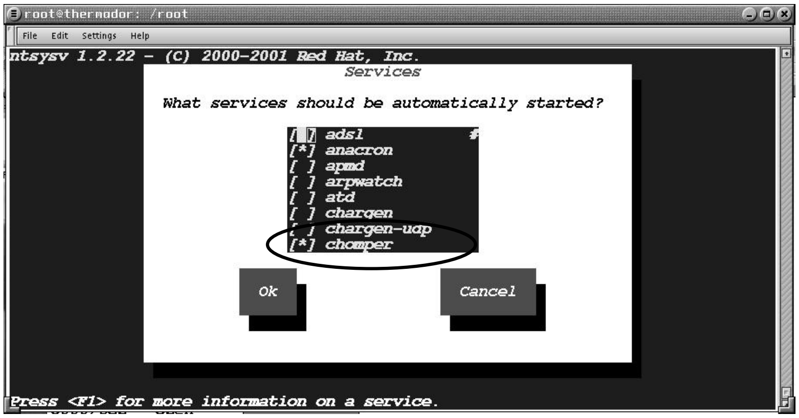
```
[root@thermador /root]# nmap 10.100.29.138

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (10.100.29.138):
(The 1512 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
79/tcp     open        finger
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
443/tcp    open        https
515/tcp    open        printer
1234/tcp   open        hotline
6000/tcp   open        X11

Nmap run completed -- 1 IP address (1 host up) scanned in 21 seconds
[root@thermador /root]# 
```

service startup

ntsysv allows check/uncheck control of service start



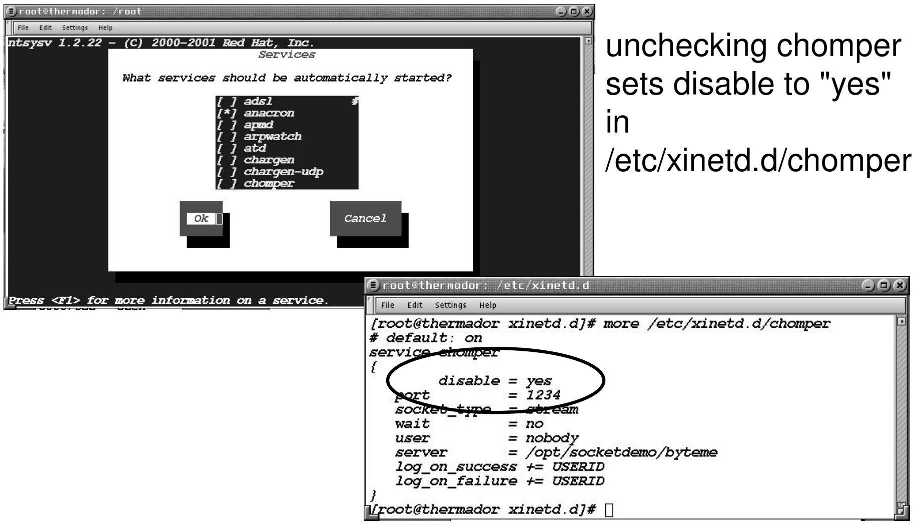
```
ntsysv 1.2.22 - (C) 2000-2001 Red Hat, Inc.
                        Services

    What services should be automatically started?

                 [ ] adsl            #
                 [*] anacron
                 [ ] apmd
                 [ ] arpwatch
                 [ ] atd
                 [ ] chargen
                 [ ] chargen-udp
                 [*] chomper

Press <F1> for more information on a service.
```

what's it do??



```
ntsysv 1.2.22 - (C) 2000-2001 Red Hat, Inc.
                        Services

    What services should be automatically started?

                 [ ] adsl            #
                 [*] anacron
                 [ ] apmd
                 [ ] arpwatch
                 [ ] atd
                 [ ] chargen
                 [ ] chargen-udp
                 [ ] chomper

Press <F1> for more information on a service.
```

```
[root@thermador xinetd.d]# more /etc/xinetd.d/chomper
# default: on
service chomper
{
        disable = yes
   port         = 1234
   socket_type  = stream
   wait         = no
   user         = nobody
   server       = /opt/socketdemo/byteme
   log_on_success += USERID
   log_on_failure += USERID
}
[root@thermador xinetd.d]# 
```

unchecking chomper sets disable to "yes" in /etc/xinetd.d/chomper