

Security Tips 1

Tip 1. Find all files that have read and write attributes

```
/usr/bin/find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg {} \;
```

Tip 2. Howto Check FreeBSD Active Ports

```
#sockstat -4  
or  
#netstat -Lan
```

Tip 3. FTPD chroot to a specific directory

If you want to restrict access to ftp users to a specific directory then create/edit your `/etc/ftpchroot` with the following content: (assuming you want to restrict user john to his `/home/john` directory)

```
# content of /etc/ftpchroot  
john /home/john ./
```

After editing `ftpchroot` file restart your `ftpd` server.
`/etc/rc.d/ftpd stop`
`/etc/rc.d/ftpd start`

Tip 4. Limit your unsuccessful SSH attempts to your server

There is a `freebsd` port that does that: `/ports/security/denyhosts/` .

```
# cd /ports/security/denyhosts/  
# make install
```

This tool will add sites in your `/etc/allow.hosts` (with block rules). You can setup the program to release that denied hosts after a period of time. The only problem that could rise if you have a lot of `ssh` traffic, your `/etc/hosts.allow` can be very large.

There is also other program in ports, that might help you: `/usr/ports/security/bruteblock`.