Basic Unix Security

- **'root' account is the master key to your system**

- **'root' password should be unguessable** (contains digits, symbols etc). **Not in any dictionary**
  – *including hackers' dictionaries!*

- **Disable root logins over telnet and modems lines: remove from /etc/securetty**
  – *you can still be root remotely by using 'su'*

- **Disable root access to FTP, POP3 and other accessible servers**
  – *Add root to* **/etc/ftpusers**
  – *Use a POP daemon which blocks root*
  – *Otherwise you have left a way for hackers to probe for the root password*

"TCP WRAPPER" (tcpd)

- **Invoked from /etc/inetd.conf instead of the daemon itself**
- **Checks access rules before starting the daemon**
- **Logs all accesses**

  e.g. /var/log/secure (see /etc/syslog.conf)

EXAMPLE CONFIGURATION

/etc/hosts.allow

```
ALL:    200.10.194.    .btl.net
ipop3d: ALL
```

/etc/hosts.deny

```
ALL:    ALL
```

see **man 5 hosts_access**

- **Relies on source IP and/or hostname**

– do we trust them?