

**passwd**

**[ian.mcloughlin@gmit.ie](mailto:ian.mcloughlin@gmit.ie)**

## passwd

```
joeb:x:1000:1000:Joe Bloggs:/home/joeb:/bin/bash
```

**/etc/passwd** stores information about users for logins.

**Passwords** are not stored in it.

**Historically** passwords were stored in the x part.

**All users** have read (but not write) access to passwd.

**Shadow** passwords are now used instead.

## shadow

```
joeb:salt+hashedpasswordhere:17895:0:99999:::
```

**/etc/shadow** stores users hashed passwords.

**Normal users** cannot read the file, only root users.

**Not perfect** but another layer of security.

**Why** not just do this to passwd?

## Hashing passwords

`$1$ie$sVz1F54.Tz0JuVRDJ3PiK.`

**1** means MD5 was used. We usually now use SHA512, and 1 becomes 6.

**ie** is the salt. It makes dictionary cracking more difficult.

**Rest** is hashed password, but with some techniques like key stretching added.