Users And Groups

Security Model

- Two Types of user
  - root
  - Everybody else
- Groups
  - Way of granting rights to a set of users

User Names and IDs

UID (User ID)

- Integer used by the system to identify a user
- Magic value of **0**, to identify **root**
- By convention we start regular users at 500 (or an other “large” number)

Name

- Human readable string
- Used by the system to display a users name
- **Usually** a one-to-one mapping with UID

Why ?

- Efficiency
  - Space
  - Speed

How ?

/etc/passwd

- Text file (a.k.a *flat file)*
- Maps UID to User Name (and more)
- Must be readable by all users

/etc/passwd

Sample Entry

```
alice:$1$NlQf1.57$CawE7UrOYp5LXxxzsvGA0:500:500::/home/alice:/bin/bash
```

Fields

name:passwd:UID:GID:comment:directory:shell

Note: passwd field is encrypted with a “one way hash”

Problem…

The passwd field is hashed, but with a well known algorithm.

Any user can see and other users hashed passwd…

Hint: John the Ripper

Solution

Leave /etc/passwd “world readable”, place just the passwd field in a file only root can read

```
$ ll /etc/passwd
$ ll /etc/shadow
```

```
# grep alice /etc/passwd
# grep alice /etc/shadow
```

/etc/shadow

Sample Entry

```
root:$1$NlQf1.57$CawE7UrOYp5LXxxzsvGA0.::0:99999:7:::
```

Format

name:hash:aging_data

See **`man 5 shadow`** for more details

Becoming An Other User

Commands:

```
su
su -
ssh <user>@localhost

sudo
```

Temporary root Access with SETUID

```
# ll /usr/bin/passwd
-rwsr-xr-x. 1 root root 25980 Feb 22  2012 /usr/bin/passwd
```

SetUID bit

Groups

- Every user may be a member of 1 or more groups
- Way of allowing a set of users access to files
- Stored in **/etc/group** and **/etc/gshadow**

User Private Groups

- Classically every user was a member of the ‘users’ group, this led to unintended sharing
- Most distributions now make each user a member of a user private group by default
- Automatically created when adding a user to the system

Managing Users And Groups

Commands

- useradd
- usermod
- groupadd
- gpasswd
- passwd

Note: Never edit the files directly

Let's try some examples