LinuxChix Africa

UNIX BASICS

To r00t or not to r00t

- Unix security is (in most cases) binary. Either you are root or you are not.
  - Effects on permissions
- Windows comparison with no users (win 3.x) to “kinds of users” i.e administrator(s) etc.
- Group permissions in UNIX also available using /etc/group

Safety Regulations

- Have a non root user for non privileged operations. (use pw useradd to add a user)
- Use su when you need root.
- Do NOT leave a root user logged in
- Chose root password (as with any other password) particularly carefully.
- (Other security considerations covered elsewhere)

Work Sheet Exercise 1

User Management

Filesystem

- Recap: no drives on system – only one huge filesystem (set of directories and files).
- Physical (or otherwise) devices are attached to the system with the “mount” command (read the man page)
- To detach devices from the filesystem we use the “umount” command. (read the man page)
- mount with no options lists the mounted systems.
- Check UNIX handout for other filesystem commands.

Work Sheet Exercise 2

- ***Attaching and Detaching devices:***

Package Management

- Easy way to install, programes are precompiled – quick to manage.
- Has a few problems:
  - Compiler optimisations absent
  - Optional features may not exist e.g. Database support.
- FreeBSD is to pkg_* as RedHAT is to rpm ... almost.
- pkg_info, pkg_add, pkg_delete etc (read man pages)

Work Sheet Exercise 3

Binary Package Management

Editors

- Most common is vi only that it has lots of modes that are interesting.
  - [ESC] key to go to command mode from any mode
  - 'i' key from command mode to start editing text
  - Refer to UNIX command reference
- ee is also another common UNIX editor – not always avaiable on some systems (e.g in single user mode to be discussed later)
  - Commands are executed using the [CTRL]+<somekey>
  - Help screen displayed in editor

Work Sheet Excercise

Enabling SSH