Edinburgh Napier UNIVERSITY

CSN08101
Digital Forensics
Lecture 1B: Essential Linux and Caine

Module Leader: Dr Gordon Russell
Lecturers: Robert Ludwiniak

Edinburgh Napier UNIVERSITY

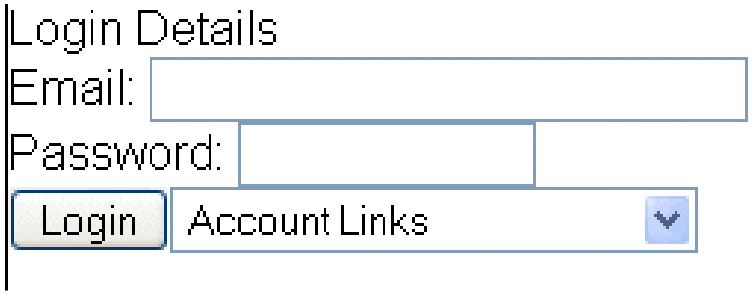
Essential Linux and Caine

You will learn in this lecture:

- Essential Command Line Linux
- Basics of the GUI and Caine environment.

Edinburgh Napier UNIVERSITY

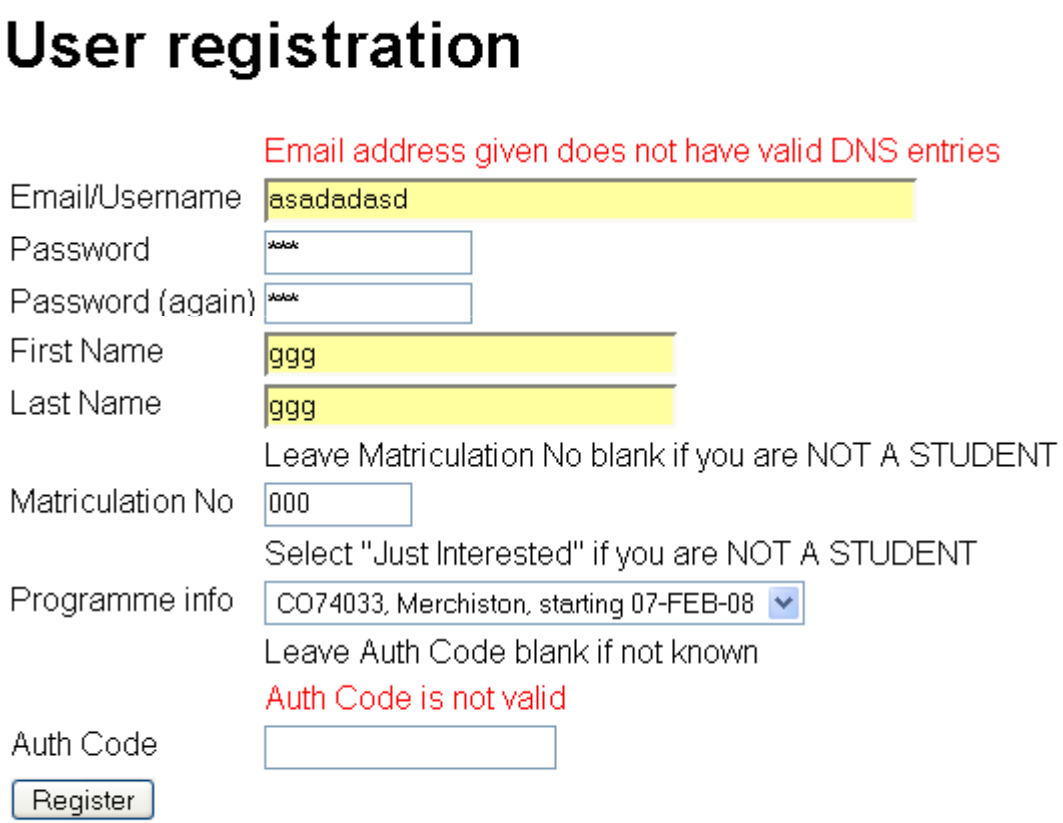
Running the Virtual Machines



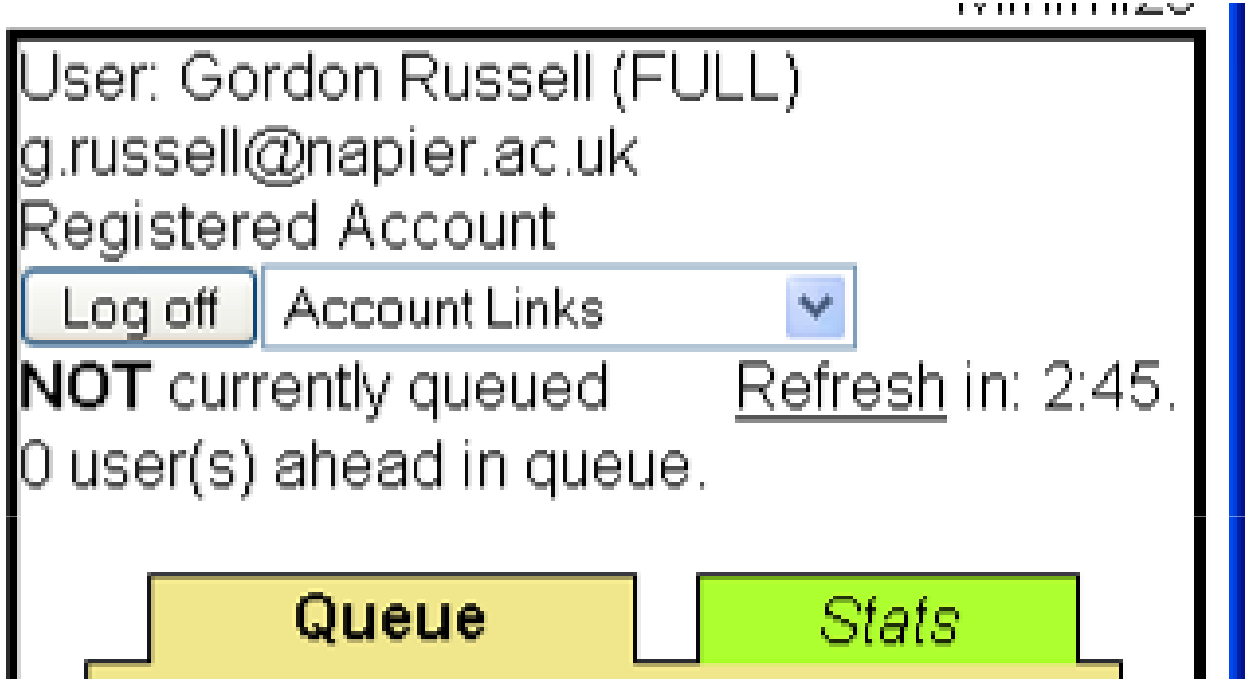
- Visit http://linuxzoo.net/
- Change the drop-down in the control box to “Register for an account”
- Read the instructions and click the link at the bottom.
- You must provide your email address, name, matriculation number, and correctly select your programme.
- Get the AUTH CODE from the lab tutor.

Edinburgh Napier UNIVERSITY

User Registration



Red means it went wrong. If you are still on this page when you click “Register” then it went wrong.

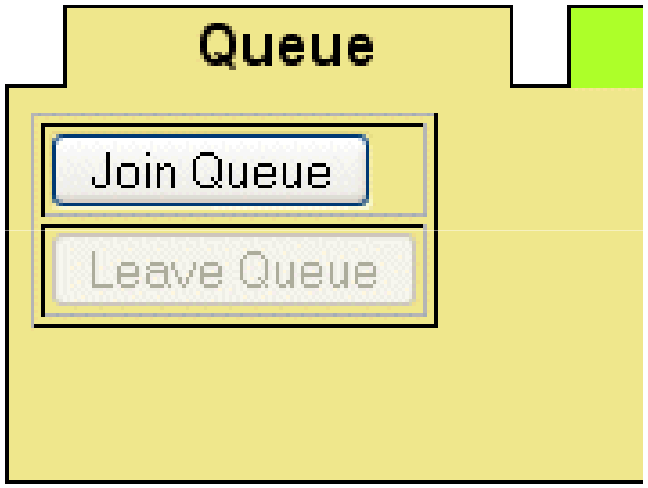


FULL) means your auth code worked. (GUEST) means you need “Your Profile” then re-enter the auth code. Without the code you may get less system time and a poor queue position.

- This is the control panel.
- You MUST ALWAYS have at least 1 window open in linuxzoo.
- If you navigate all windows away from linuxzoo you will be logged out.

Edinburgh Napier UNIVERSITY

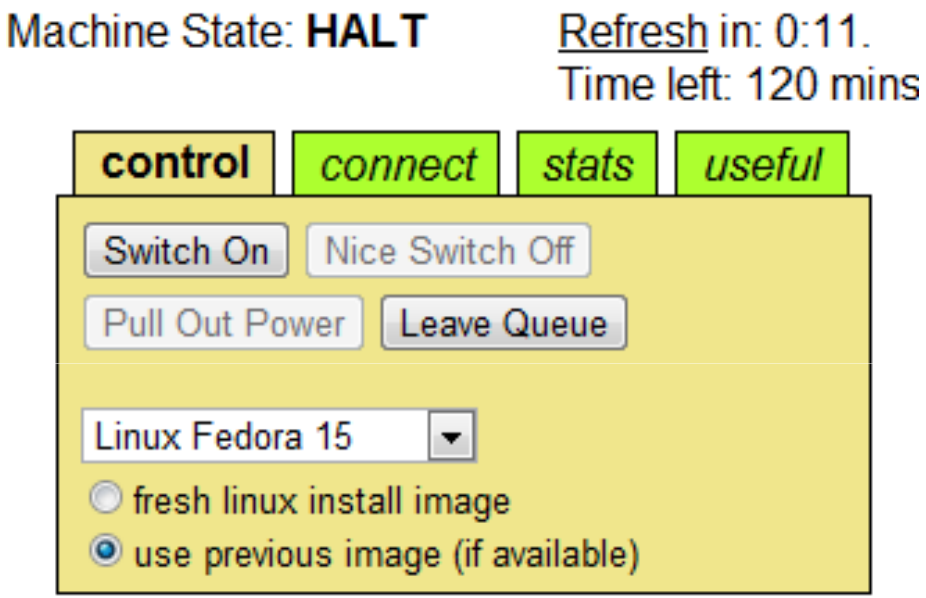
Queue for a machine



- Once logged in Join the Queue.
- During busy period you may have to wait in the queue for a while...

Edinburgh Napier UNIVERSITY

Boot the machine



- HALT is the same as OFF. You need to switch the machine on.
- Make sure you choose “Linux Fedora 15”.

Edinburgh Napier UNIVERSITY

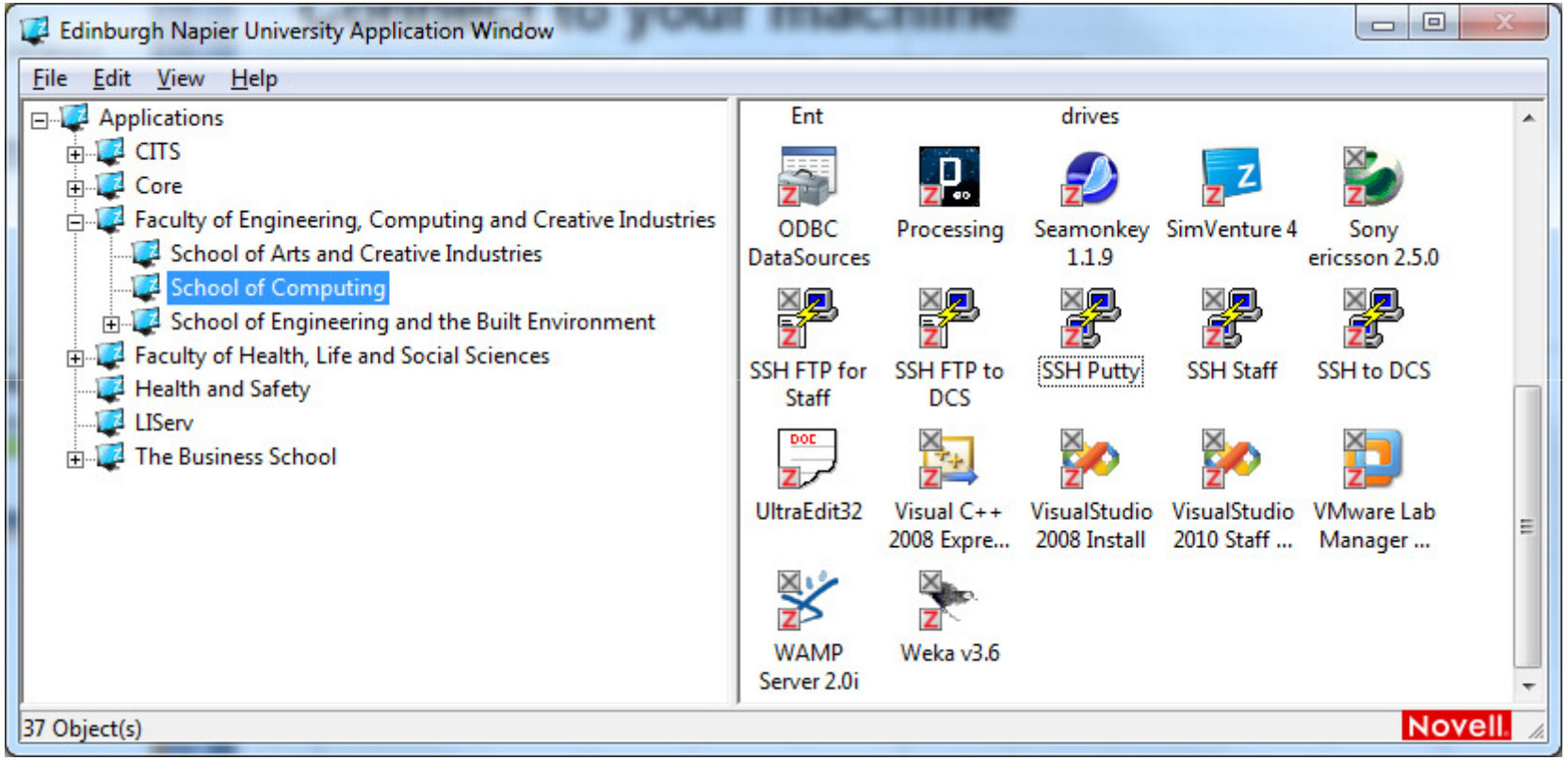
Booting takes time

Edinburgh Napier UNIVERSITY

Connect to your machine

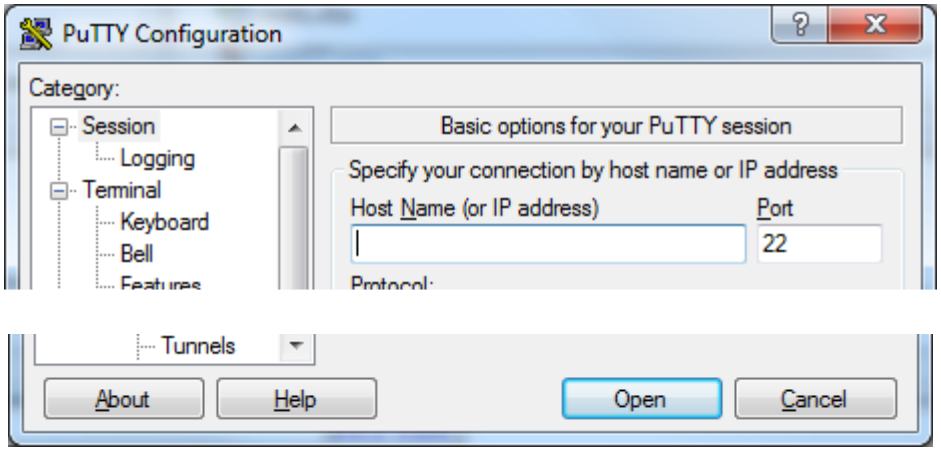
- You can have Java Telnet and JavaScript Telnet from here.
- But better to have a real telnet or ssh client.
- You can download an excellent ssh client from the web called putty. http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html then download putty.exe

Putty in the JKCC



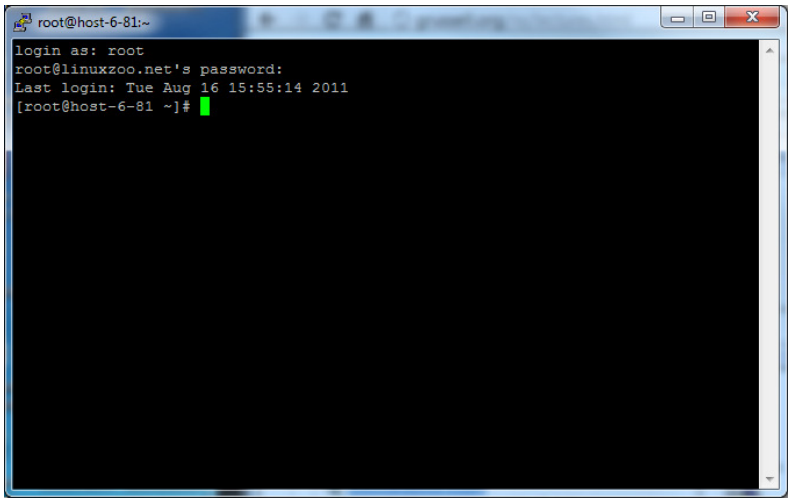
- It is “SSH Putty”.

Putty login



- Hostname is “linuxzoo.net”.
- Then click Open

- Administration username is “root” and password is “secure”.
- When created the demo account is password “demo”.



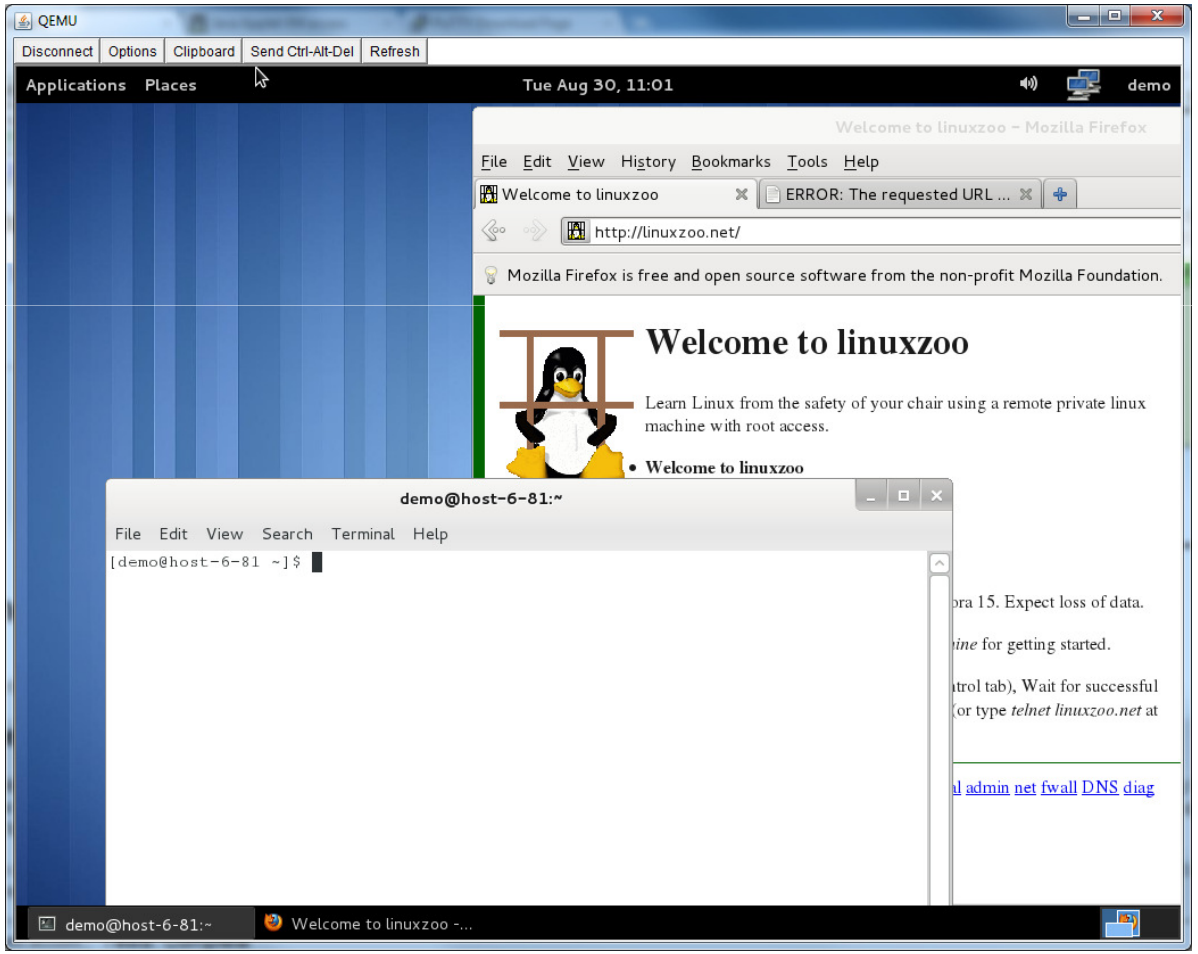
Edinburgh Napier UNIVERSITY

Why A Command Prompt?

- Linux does have a graphical interface.
- However it is faster, easier, and more powerful to use commands at a prompt to configure a server.
- Commands do mean a steep learning curve.
- Editing is tough!
- You can have a graphical interface by clicking on “Java VNC” in the connect tab of the control panel.
  - You need Java installed!
  - Sometimes when you release a key that event is lost. This causes the last key pressed to repeat infinitely. Just press another key to fix the problem.

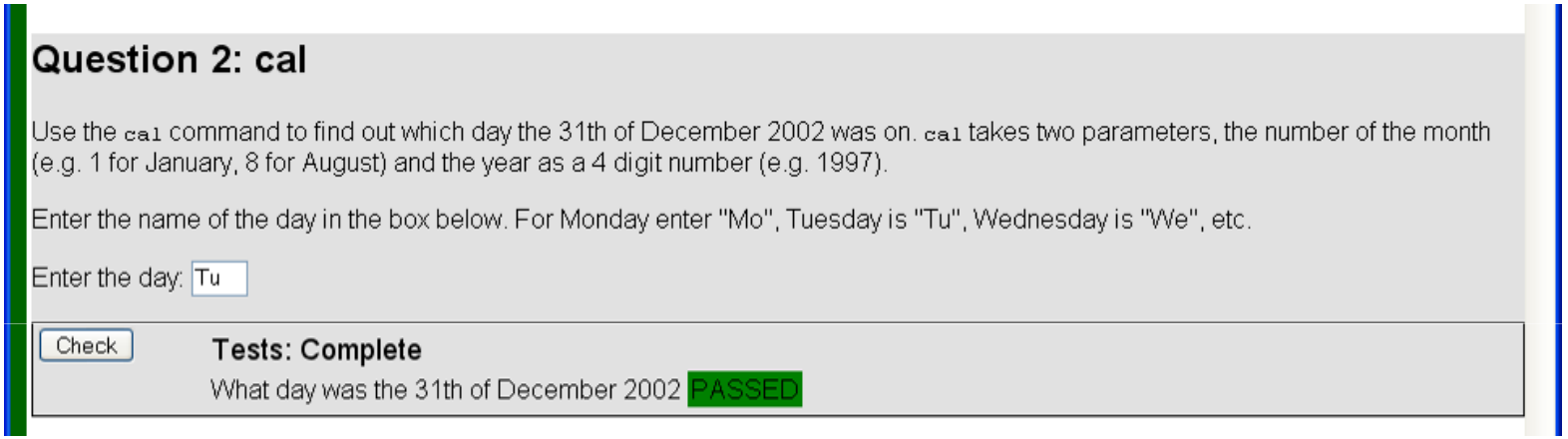
Edinburgh Napier UNIVERSITY

The VNC of Fedora 15



Edinburgh Napier UNIVERSITY

The Tutorials.



Edinburgh Napier UNIVERSITY

Tutorials Username

- The Caine environment has a user called “caine” with password “caine”.
- If you need to run a “root” administration command you need to use “sudo”. This is explained in the practicals.

Edinburgh Napier UNIVERSITY

Running a tutorial Machine

- Your machine is a VIRTUAL machine.
- Your VM uses a shared computer resource.
- The resource is limited!
- Do not go crazy (do not recompile the world).
- Priority goes to those in timetabled labs.
- Your virtual disk is not reliably preserved between sessions. Do not save your life work on it.

Edinburgh Napier UNIVERSITY

The Basics

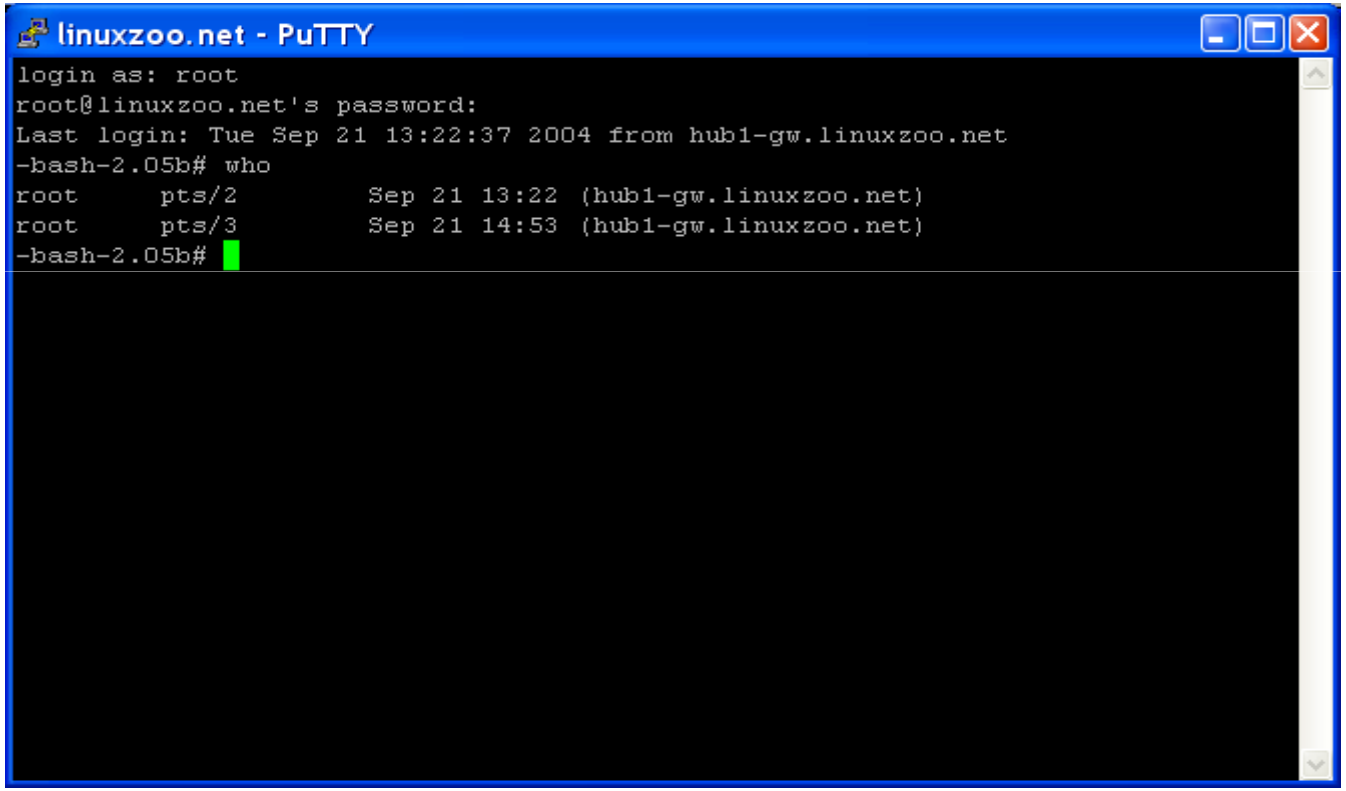
- Before your machine operates it must BOOT.
- As it boots things are started up.
- Only when the boot process completes will the system be fully operational.
- When you are finished, a machine can be shutdown or halted.
  - Shutdown – does it nicely and cleanly
  - HALT – pulls the power out the back.

Edinburgh Napier UNIVERSITY

Connecting to Caine

- VNC gives you the graphical desktop.
  - Good in general but hard to cut-and-paste between the virtual machine and your own machine
  - CTRL C may cause a strange key repeat problem.
  - Needs Java Applets and support for HTTP CONNECT.
- telnet is old-fashioned but is often installed in older Oses.
  - No graphic support but low bandwidth.
  - Easy cut and paste.
  - Needs TCP port 23.
- Ssh is new-world.
  - No graphic support but low bandwidth
  - Very easy cut and paste
  - Needs TCP port 22.
- Best to use a mix of interfaces to get the best overall experience.

Edinburgh Napier
UNIVERSITY



Basic Commands

- To see the files and directories in a directory use the “ls” command.
- Sometimes pronounced “list”.

- Examples:

$ ls

```
Desktop  dir1  f1  my1  thedir  thefile
```

$ ls -a

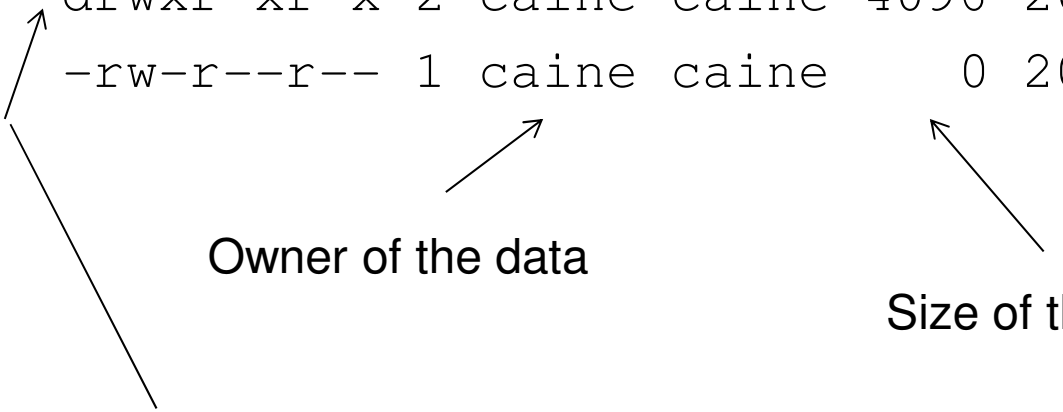
```
.               .esd_auth         .gvfs                .sudo_as_admin_successful
..              .evolution        .ICEauthority        thedir
.bash_history   f1                .icons               thefile
.cache          .fontconfig       .local               .themes
.config         .gconf            my1                  .thumbnails
.dbus           .gconfd           .nautilus            .update-notifier
Desktop         .gksu.lock        .pulse               .xsession-errors
dir1            .gnome2           .pulse-cookie        .xsession-errors.old
.dmrc           .gnome2_private   .recently-used.xbel
```

Long listing

$ ls -l

total 16

```
drwsrwsrwt 2 caine caine 4096 2012-01-10 13:21 Desktop
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 dir1
-rw-r--r-- 1 caine caine    0 2012-01-19 11:29 f1
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 my1
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 thedir
-rw-r--r-- 1 caine caine    0 2012-01-19 11:29 thefile
```



Edinburgh Napier UNIVERSITY

Directory Traversal: cd and pwd

```
$ pwd
/home/caine
$ cd ..
$ pwd
/home
$ cd /home/caine
$ pwd
/home/caine
$ cd dir1
$ pwd
/home/caine/dir1
```

Directory Creation

Edinburgh Napier UNIVERSITY

$ pwd

/home/caine

$ mkdir newdir

$ ls –l

```
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 my1
drwxr-xr-x 2 caine caine 4096 2012-01-19 12:37 newdir
-rw-r--r-- 1 caine caine    0 2012-01-19 11:29 thefile
```

$ cd newdir

$ pwd

/home/caine/newdir

$ cd ..

$ pwd

/home/caine

Directory Removal

Edinburgh Napier UNIVERSITY

$ pwd

/home/caine

$ rmdir newdir

rmdir: failed to remove `newdir': Directory not empty

$ ls newdir

d2

$ rm –rf newdir

- “r” is recursive and “f” is force.
- Use care, as this can delete everything from the top to the bottom of a directory tree without prompting “are you sure”!

Edinburgh Napier UNIVERSITY

cd ..

- If you are in a directory and you want to go to the parent, use “..”

$ pwd

/home/caine

$ cd ..

$ pwd

/home

Edinburgh Napier UNIVERSITY

cd ../..

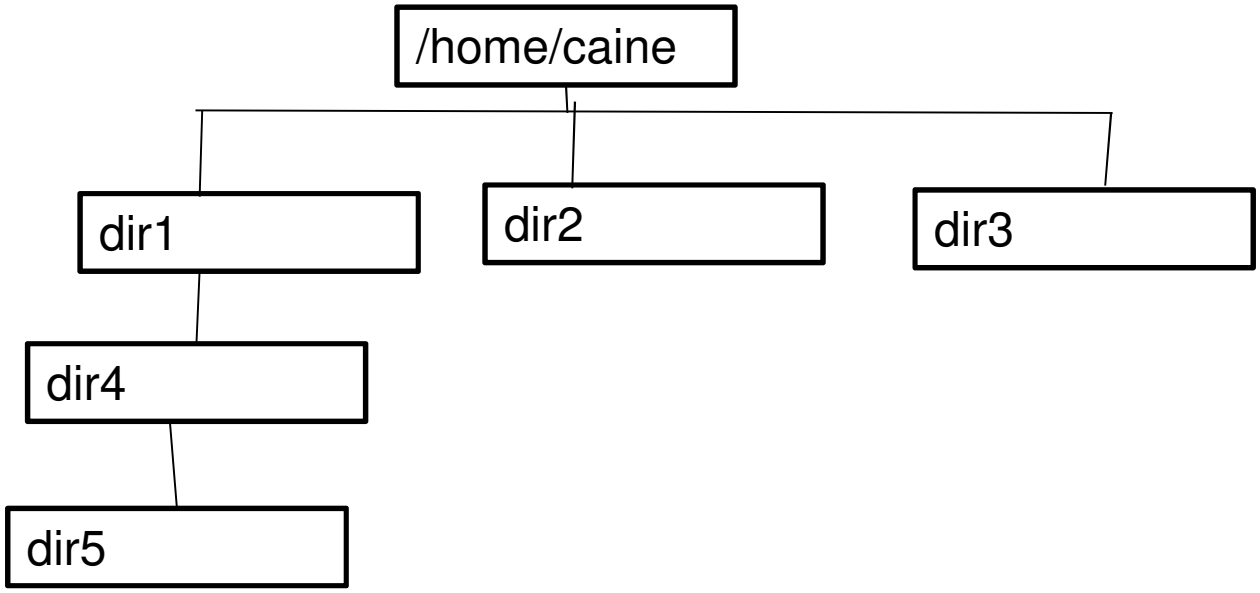
- You can navigate multiple steps in one go using “/”

```
$ pwd
/home/caine/dir1
$ cd ..
$ pwd
/home
$ cd caine/dir1
$ pwd
/home/caine/dir1
$ cd ../../caine
$ pwd
/home/caine
```

Edinburgh Napier UNIVERSITY

Assessment: Short-Answer Examples

- Specify the commands to create the following directory tree in /home/caine



Edinburgh Napier UNIVERSITY

```
$ cd /home/caine
$ mkdir dir1
$ mkdir dir2
$ mkdir dir3
$ mkdir dir1/dir4
$ mkdir dir1/dir4/dir5
```

```
$ cd /home/caine
$ mkdir dir1
$ mkdir dir2
$ mkdir dir3
$ cd dir1
$ mkdir dir4
$ cd dir4
$ mkdir dir5
```

```
$ cd /home/caine
$ mkdir dir1 dir2 dir3
$ mkdir dir1/dir4
$ mkdir dir1/dir4/dir5
```

Edinburgh Napier UNIVERSITY

What is the biggest file?

```
drwsrwsrwt 2 caine caine 4096 2012-01-10 13:21 Desktop
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 thing3
-rw-r--r-- 1 caine caine 4095 2012-01-19 11:29 thing2
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 my1
drwxr-xr-x 2 caine caine 4096 2012-01-19 11:29 thedir
-rw-r--r-- 1 caine caine   50 2012-01-19 11:29 thefile
```