CSN11121
System Administration and Forensics
Week 2: Introduction/Linux Basics

Module Leader: Dr Gordon Russell
Lecturers: G. Russell, R.Ludwiniak

Aliases: CSN11122 (Distance Learning Version)
System Administration and Forensics

• Focus on host based forensics from a Linux platform.
• Covers:
  – Basic Linux Commands
  – Some administration issues pertinent to forensics.
  – The use of Caine for host-based forensics
  – The theory behind host-based forensics.
• Uses “linuxzoo.net” for practical exercises.
• Pre-requisites for this module are:
  – Basic OS concepts (partitions, virtual memory, processes, etc).
• This module is known as
  – CSN11121 (normal version of module)
  – CSN11122 (distance learning version of the module)
Why Linux

• Linux is a powerful operating system.
  – Many web sites use Linux as the operating system
  – Even Steve Ballmer of Microsoft said Linux has 60% of the server market in 2008.
  – Tolerant of a range of hardware platforms without special configuration.
• Computer Forensics need to be able to consider server forensics.
  – Forensic issues can happen on server platforms too.
• Host-Based forensic tools often run on linux platforms.
  – Free platform
  – Flexible and reliable
  – Easier to access low-level interfaces
  – Good forensic qualities.
  – Will consider Caine (a Linux live cd) for host-based forensics, which runs The Forensic Toolkit and Autopsy.
Module Split

• This module is in 2 parts:
  – Server Administration
  – Host Based Forensics
• The first 6 weeks is on Server Administration.
• Linux assessed using a supervised class test demonstrating practical knowledge of linux.
• The host-based forensics component of the module is assessed by a coursework report submitted at the end of the trimester.
• This material only considers the Linux component of the module.
Recommended Linux Reading

• Variety of good books on system administration.

• Recommended book for general admin:

  UNIX SYSTEM ADMINISTRATION HANDBOOK:
  Third Edition – EVI NEMETH et all

• However any Linux book is probably good.
  – Redhat/Fedora is the market leader for the Server Market
  – Ubuntu/Debian is a strong contender for the desktop market.
  – Caine uses Ubuntu.
Elements Covered

• The module covers some important aspects of system administration for Linux machines:
  – Basic Unix / command prompt
  – Linux user administration.
  – Basic Apache Web Server administration and Log Analysis.
  – Linux Hacking and Security Techniques
Timetable

• **Attending Students:**
  – You should attend 2 hours of lectures + 2 hours of practicals per week.
  – Lectures will be mostly “lecturing”, but will also include group tutorial sessions.
  – Practicals are all online, but you should still attend practical sessions as timetabled.
  – Personal time is also required (e.g. 10 hours/week).
  – There is a forum to help you too.
  – Attendance will be taken.

• **Distance Learning Students:**
  – Put aside a significant period per week for study (e.g. 14 hours per week)
  – Lecture slides and summary notes are available online.
  – Online lectures will be prepared and supplied where possible.
  – Complete practicals as per the attend students schedule.
  – Use the forums for questions and discussions.
Tutorials

- These run using any networked PCs.
- Tutorials involve you being the administrator on your own Linux machine.
- This is available online from http://linuxzoo.net

This is an in-house system, and in some ways an experimental system, and this is also a new module. I expect that there may be initial technical problems to be fixed. I would appreciate your patience and constructive feedback.
Lectures

- The lectures are 1-2 hours long.
- Lectures are not the source of all knowledge.
- You need to do some reading on your own, and to practice with the Linux machines.
- If you don’t attend the tutorials and lectures, and practice what you have learned right from the first week, you may struggle with this module.
# Weeks 2 – 6 (Linux)

<table>
<thead>
<tr>
<th>Week</th>
<th>Lecture</th>
<th>Class</th>
<th>Tutorials</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Intro / Linux basics</td>
<td>Use of Linux</td>
<td>intro1 intro2</td>
</tr>
<tr>
<td>3</td>
<td>Users, Permissions, Processes, Pipes</td>
<td></td>
<td>wildcard permission</td>
</tr>
<tr>
<td>4</td>
<td>Basic Administration Concepts</td>
<td></td>
<td>pipe vi</td>
</tr>
<tr>
<td>5</td>
<td>Basic Apache + Logs</td>
<td></td>
<td>Essential (not Q8,10,11), diag</td>
</tr>
<tr>
<td>6</td>
<td>Hacking + Security</td>
<td></td>
<td>Apache1, Q1-4</td>
</tr>
</tbody>
</table>
# Weeks 7 – 14 (host-based forensics)

<table>
<thead>
<tr>
<th>Week</th>
<th>Lecture</th>
<th>Tutorials</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Introduction to Forensics</td>
<td>** Linux PRACTICAL EXAM **</td>
</tr>
<tr>
<td>8</td>
<td>Storage Devices and File Systems</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Partition Information and File Metadata</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Windows Registry</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Timeline Analysis</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Web Browsing Forensics</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Case Study: Anti-Forensics</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Report Due</td>
<td>Not Scheduled</td>
</tr>
</tbody>
</table>
Practical Assessment

- Practical Assessment for Linux:
  - In-Class OPEN BOOK timed assessment.
  - This will happen in week 7.
  - 1-2 hour Linux network and Linux configuration and troubleshooting.
  - This is worth 50% overall

- A capped resit attempt is offered if you fail the practical
  - Submission is in week 13. Max score is half marks.
  - It is an essay based coursework.
Running the Virtual Machines

<table>
<thead>
<tr>
<th>Login Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
</tbody>
</table>

- 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.
User Registration

User registration

Email address given does not have valid DNS entries
- asadadasd

Password
- 

Password (again)
- 

First Name
- ggg

Last Name
- ggg

Leave Matriculation No blank if you are NOT A STUDENT
- 000

Select "Just Interested" if you are NOT A STUDENT

CO74033. Merchiston, starting 07-FEB-08

Leave Auth Code blank if not known

Auth Code is not valid

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

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.
Queue for a machine

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

- HALT is the same as OFF. You need to switch the machine on.
- Make sure you choose “Linux Fedora 15”.
Booting takes time
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](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) then download putty.exe
Putty in the JKCC

- It is “SSH Putty”.

[Image of a computer screen showing the folder structure and applications, including 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”.

![PuTTY Configuration](image1)

![Putty login interface](image2)
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.
The VNC of Fedora 15
Unix Flavours

• There are many flavours of unix and Linux.
• Linux “distributions” include:
  – Fedora
  – Redhat
  – Novell SUSE
  – Gentoo
• Different distributions have things in common but some differences. The distributions selection is often down to personal choice and “what my friend uses”.
Telnet in the virtual machines

- Telnet is quite clever and usually no matter what OS and keyboard you have things just seem to “work”.
- Sometimes however telnet gets confused.
- If you ever have a problem where cursor keys stop working, or your editor corruptions the screen try these magic commands (you don’t type the “>”):
  
  > export TERM=vt100
  
  > tset
The Tutorials.

**Question 2: cal**

Use the `cal` command to find out which day the 31st of December 2002 was on. `cal` takes two parameters, the number of the month (e.g. 1 for January, 8 for August) and the year as a 4 digit number (e.g. 1997).

Enter the name of the day in the box below. For Monday enter "Mo", Tuesday is "Tu", Wednesday is "We", etc.

Enter the day: **Tu**

Tests: Complete

What day was the 31st of December 2002? **PASSED**
Tutorials Username

- The advanced tutorials use the root user (password secure).
- The basic tutorials create a user called “demo”, password “demo”.
- If you are not logged in you can just log in as demo.
- If you are logged in as root:
  > su - demo
  Demo> ..... 
  Demo> <CTRL><D> 
  >
Useful commands:

- `ls`
- `cat`
- `cal`
- `date`
- `pwd`
- `more`
- `cd`
- `mkdir`
- `cp`
- `mv`
- `rm`
- `rmdir`
- `man`
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.
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.
login as: root
root@linuxzoo.net's password:
Last login: Tue Sep 21 13:22:37 2004 from hub1-gw.linuxzoo.net
-bash-2.05k# who
root pts/2 Sep 21 13:22 (hub1-gw.linuxzoo.net)
root pts/3 Sep 21 14:53 (hub1-gw.linuxzoo.net)
-bash-2.05k#
The PROMPT

• Once you log into your machine, you are at the prompt. Here you can perform your commands.
• Everything on Linux is either a file or a directory.
• A file which is executed becomes a process.
• Processes can be seen as files too.
• Devices, such as scanners and hard drives are also files.
> ls /

    bin  dev  home  lost+found  mnt  root  selinux  
    tmp  var  boot  etc  lib  misc  proc  sbin  
    sys  usr

- Directories use / in linux (like Windows uses \).
- No volumes in linux (like C: or A: )
- / is called the root directory.
- ls splits the files either by line or in this case by tabs.
Directories

- /bin: This contains commands a user can run, like ‘ls’, but which might be needed during boot.
- /dev: This contains devices, like the mouse.
- /home: This is where users store their files.
- /tmp: Temporary storage for users and the system.
- /var: System files which can change.
- /etc: System config files which don’t change.
- /lib: Where all the system libraries live.
- /proc: Files which represent the running system (like processes).
- /sbin: Commands which only an administrator would want.
- /usr: Commands which are never needed during bootup.
> cal

August 2008
Su  Mo  Tu  We  Th  Fr  Sa
  1   2
  3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
  31
Redirection

- If you end a command with “>”, its output goes to a file.
- If you end a command with “<”, its input comes from a file.

```
$ ls
a
$ cal > b
$ ls
a b
$ cat b

August 2008
Su Mo Tu We Th Fr Sa
  1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
```
Prompts

- When explaining commands, we usually put a prompt character before it to make it clear that the command has to be typed.
- You can set the prompt to anything, but in examples prompts like $ or > are common.
- Don’t type the first > or $ you see:
  $ ls
  $ cal
  > ls
  > cal
Parameters

- Some commands change behaviours with different parameters.
- If a parameter relates to a file, then it is called a “parameter”.
- However, if the parameter changes the behaviour of the program, it is instead called an “option” or “flag”.

Edinburgh Napier University
Flags

$ cal
   August 2008
 Su Mo Tu We Th Fr Sa
        1  2
  3  4  5  6  7  8  9
...

$ cal -m
   August 2008
 Mo Tu We Th Fr Sa Su
        1  2  3
  4  5  6  7  8  9 10
...

Edinburgh Napier UNIVERSITY
Man pages

- If you don’t know what options or flags are possible for a command, use “man”
- For instance, to find out what flags cal uses, do:
  $ man cal
- To get out of man, press “q”. Space shows you more of the information.
NAME
cal - displays a calendar

SYNOPSIS
cal [-smjy13] [[month] year]

DESCRIPTION
Cal displays a simple calendar. If arguments are not specified, the current month is displayed. The options are as follows:

-1  Display single month output. (This is the default.)
-3  Display prev/current/next month output.
-s  Display Sunday as the first day of the week. (This is the default.)
-m  Display Monday as the first day of the week.
-j  Display Julian dates (days one-based, numbered from January 1).
**Man -k**

- You can keyword search for commands
- For instance, what commands show a calendar?

```
$ man -k calendar
cal          (1)  - displays a calendar
cal          (1p) - print a calendar
difftime     (3p) - compute the difference...
```
Directories

$ ls
a  b
$ mkdir d1
$ ls
a b d1
$ cd d1
$ pwd
/home/demo/d1
$ pwd
/home/demo/d1
$ cd..
$ pwd
/home/demo/
$ ls
a  b  d1
$ rmdir d1
$ ls
a  b
Directory characters

• Absolute location (Starts with “/”)
cat /home/demo/z1
cat ~demo/z1

• Relative location (where z2 is a directory)
cd /home
cat demo/z1

cd /home/demo/z2
cat ../z1
Wildcards

- Parameters which match filenames don’t have to be complete. You can pattern match with the characters “?” for a single character and “*” for a number of characters.

$ ls
aaa aab abb

$ ls aa?
aaa aab

$ ls a*
aaa aab abb
**Wildcard [set]**

- You can pattern match with a set of characters. For instance, you want files which end with a or b.

```
$ ls
aaa  aab  aac  zzb  zzc
$ ls aa[ab]
aaa  aab
$ ls *[ab]
aaa  aab  zzb
```
Tutorials Week 2

• You should now be able to complete
  – Intro1
  – Intro2
  – Wildcard (not links)
Discussions

- Who is using Linux?
Discussions

• What is Linux for?
  – Desktop
  – Software Developers
  – Servers