Linux Fundamentals

Overview

- Core concepts of Linux operating system
- The Linux Shell
- User Account Management
- Mounting Drives
- Tarballs and Zips
- Installing programs
- Linux Distributions and Live CDs/DVDs

Linux History: Linus + Minix = Linux

In the spring of 1991, Linus Benedict Torvalds, a Finnish student, began to take a closer look at the memory management of his 386 PC.

A few months later he had developed a rudimentary kernel that he passed on as a source text to others who were interested via the Internet.

The GNU Operating System

This information can be found at http://www.gnu.org/

- Richard Stallman started the project.

The GNU Project was launched in 1984 to develop a complete UNIX like operating system which is free software: the GNU system.

GNU is a recursive acronym for “GNU's Not UNIX”; it is pronounced “guh-noo,”.

Variants of the GNU operating system, which use the kernel Linux, are now widely used; though these systems are often referred to as “Linux”, they are more accurately called GNU/Linux systems.

Linux Introduction

Open Source Operating system is free although some distros are for sale – Redhat & SuSE are two examples

Largely used in schools, colleges & universities.

Most popular system used by hackers.

Some believe it is the most attacked operating system due to the availability of the source code.

However, the "open source community" quickly finds and resolves exploits.

Linux GUI Desktops

KDE - (K Desktop Environment) is a free desktop environment and development platform built with Trolltech's Qt toolkit. It runs on most Unix and Unix-like systems, such as Linux, BSD, AIX and Solaris. There are also ports to Mac OS X using its X11 layer and Microsoft Windows using Cygwin.

GNOME (GNU Network Object Model Environment) is an international effort to create an easy-to-use computer desktop environment built entirely from software considered free by the Free Software Foundation.

Fluxbox - Fluxbox is a window manager for the X Window System. It aims to be lightweight and highly customizable, with only minimal support for graphical icons, and only basic interface style capabilities. The basic interface has only a task bar and a menu accessible by right-clicking on the desktop.

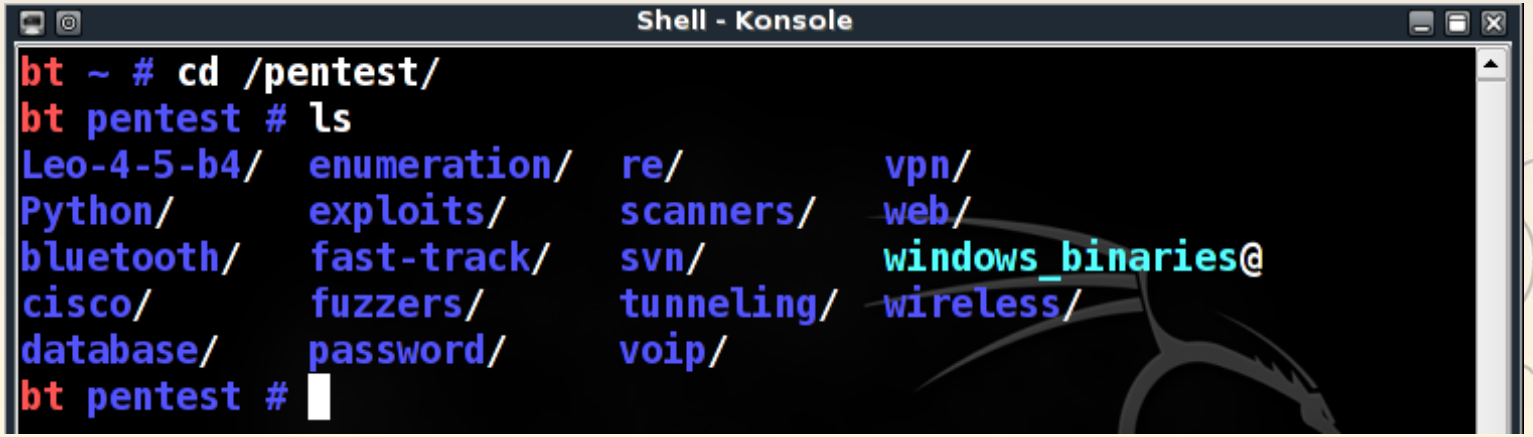
Linux Shell

Shell is a user program or it's environment provided for user interaction. Shell is a command language interpreter that executes commands. The shell is a program that acts as a buffer between a user and the operating system. It can also be used for simple programming.

Interactive Use - When the shell is used interactively, it waits for you to issue commands, processes them, and executes them. Shells also provide a set of commands to supplement Linux commands.

Customizing Your Linux Session - A Linux shell defines variables, such as the locations of your home directory and mail spool, and to control the behavior of your session. Some variables are preset by the system; you can define others in startup files, or interactively for a single session.

Programming - A series of individual commands combined into file is called a shell script. Bash is considered a powerful programming shell, while scripting in tcsh is rumored to be hazardous to your health.

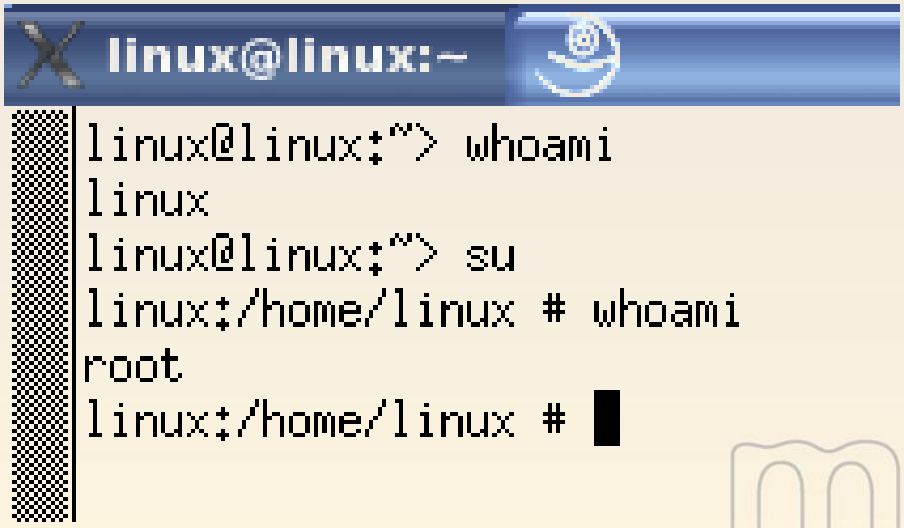


Linux Bash Shell

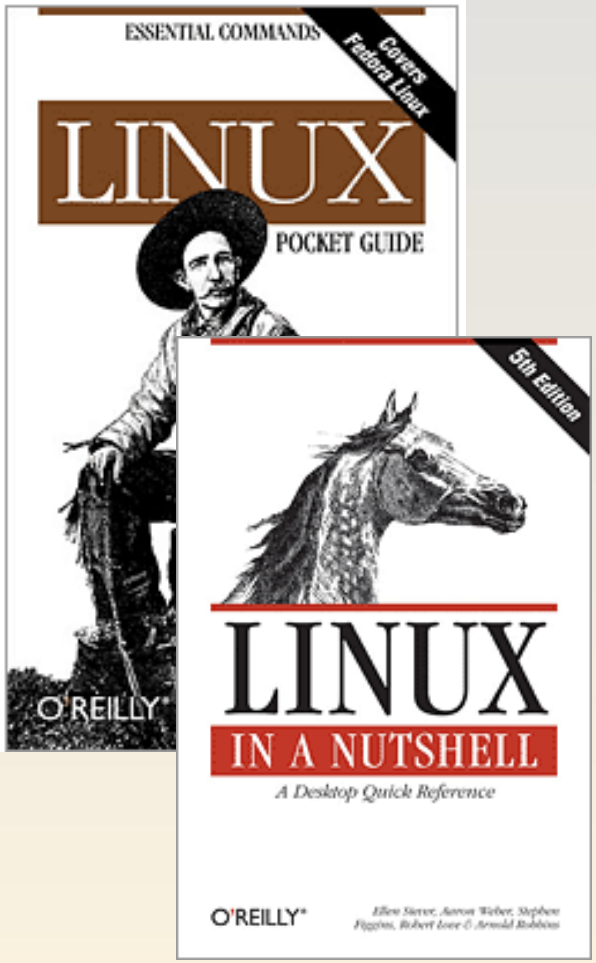
Bash is a UNIX command shell written for the GNU project. Its name is an acronym for Bourne-again shell — a pun on the Bourne shell (sh), which was an early, important UNIX shell.

To run powerful programs such as sniffers, you will need to be operating as Root. To switch to another account, type su username.

Switch to Root and you can now start programs under the security context of Root.



Recommended Linux Book



LINUX POCKET GUIDE

- Gets you up to speed quickly on day to day Linux use. The book begins with general concepts like files and directories, the shell, and X windows, and then presents detailed overviews of the most essential commands.
- ISBN 10: 0-596-00628-4

Linux in a Nutshell

- This updated fifth edition covers all substantial user, programming, administration, and networking commands for the most common Linux distributions. Considered by many to be the most complete and authoritative command reference for Linux available. No matter how you use Linux, you need the quick access to information this book provides.
- ISBN 10: 0-596-00930-5

Password & Shadow File Formats

passwd	This lists local users. Use the shadow utilities useradd, usermod and userdel to edit this file. Edit manually only when user really know what they are doing.
shadow	The shadow file holds security sensitive data of local accounts in the passwd file. Only root can alter the data in the shadow file.

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called "/etc/passwd".

As this file is used by many tools (such as "ls") to display file ownerships, etc. by matching user id numbers with the users' names, the file needs to be world-readable. Consequently, this can be somewhat of a security risk.

A more secure method of storing account information is with the shadow password format.

A second file, called "/etc/shadow", contains encrypted passwords as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk.

Password & Shadow File Formats

With shadow passwords, the "/etc/passwd" file contains account information, and looks like this:

```
smithj:x:561:561:Joe Smith:/home/smithj:/bin/bash
```

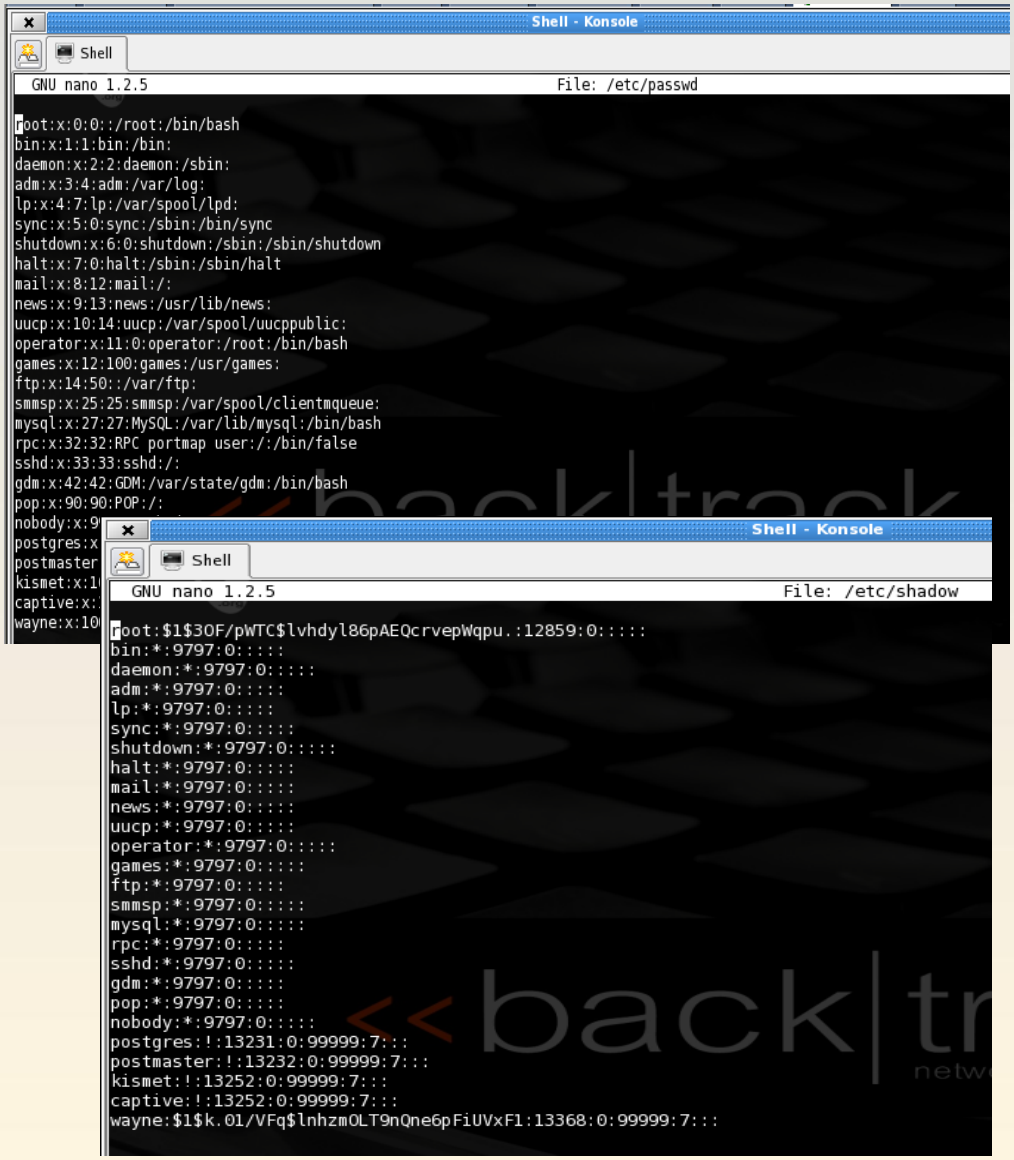
The "/etc/shadow" file contains password and account expiration information for users, and looks like this:

```
smithj:Ep6mckrOLChF.:10063:0:99999:7:::
```

User Account Management

To view your passwd file in BackTrack: nano /etc/passwd

To view your shadow file in BackTrack: nano /etc/shadow



Instructor Demonstration

Creating a new user account using BackTrack:

- **From a shell type: adduser**

Follow the prompts for adding additional account information.

Shell - Konsole

Shell

```
slax ~ # adduser

Login name for new user []: john

User ID ('UID') [ defaults to next available ]:

Initial group [ users ]:

Additional groups (comma separated) []:

Home directory [ /home/john ]

Shell [ /bin/bash ]

Expiry date (YYYY-MM-DD) []: 2006-10-01

New account will be created as follows:

---------------------------------------
Login name.......:  john
UID..............:  [ Next available ]
Initial group....:  users
Additional groups:  [ None ]
Home directory...:  /home/john
Shell............:  /bin/bash
Expiry date......:  2006-10-01

This is it... if you want to bail out, hit Control-C.  Otherwise, press
ENTER to go ahead and make the account.
```

Changing a user account password

To change another user's password, from the shell prompt type: passwd accountname

To change your own password, from the shell prompt type: passwd

Shell - Konsole

Shell

```
slax ~ # passwd john
Changing password for john
Enter the new password (minimum of 5, maximum of 127 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
```

Configuring Network Interfaces with Linux

Nearly every aspect of the network configuration can be modified with ifconfig

Root access is required to configure the network.

Display the interface configuration:

- ifconfig eth0

Turn on or off the interface:

- ifconfig eth0 down / up

Configure an IP address (default sub-net mask):

- ifconfig eth0 192.168.1.2

Configure a non default sub-net mask:

- ifconfig eth0 10.1.1.2 NETMASK 255.255.255.0

Add a default gateway to the eth0 interface:

- route add default gw 192.168.1.1 eth0

Mounting Drives with Linux

Linux stores all "devices" in the /dev directory. This lists all drives that the Linux OS can use; /dev/hda lists IDE hard drives and /dev/sda lists SCSI hard drives and removable media.

To access a drive you need to mount it with the "mount" command. All mounted drives are listed in the /mnt directory.

To mount a drive from a shell, type:

- mount <source> <destination>

You must specify a source, e.g. /dev/hda1. You should also specify an existing location to mount to, e.g. /mnt/hda1.

Now you can read the contents of the mounted drive. Linux does not natively support write access to NTFS drives although you can install software that will allow full control.

```
$ mkdir /mnt/hda1
$ mount /dev/hda1 /mnt/hda1
$ cd /mnt/hda1
$ ls
```

```
$ mkdir /mnt/sda1
$ mount /dev/sda1 /mnt/sda1
$ cd /mnt/sda1
$ ls
```

Tarballs and Zips

The "tarball" is a system that will bundle many files together, generally for compression.

To "untar" a file run the following command:

tar –xvf file.tar

A Linux program for compressing files is GZIP. Files with a .gz extension have been compressed and require uncompressing before being used.

gunzip -c /opt/file.txt.gz >/file.txt

You may find files that have been 'tarballed' and compressed.

file.tar.gz	file.tgz

In which case you should uncompress and untarball with the z switch.

tar –xzf file.tgz

Compiling Programs in Linux

GCC is a common 'C' compiler for Linux operating systems released under the GNU license agreement.

```
gcc –o program program.c
```

For standalone executables, all that is required is a compile of the program and execution with the ./ prefix.

```
./program
```

To install a program, there are generally 3 steps:

- Configuring how the program will be compiled
- Compiling the program
- Installing the program
  - $ ./configure
  - $ make
  - $ make install

Why Use Live Linux Boot CDs

Live Linux CDs allow you to boot the operating system from CD or DVD and you have access to many tools built into the CD/DVD in a compressed format.

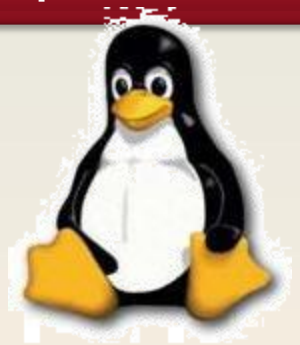
You can:

Try Linux without installing it

Use as a portable and secure desktop as you have only read access unless you set up a persistent Ram disk

Reset forgotten Windows passwords

Scan safely for malware



Typical Linux Operating Systems

http://www.linux.org/dist/list.html

slackware linux

redhat

gentoo linux

fedora

FreeBSD The Power To Serve

ubuntu

debian

Mandriva

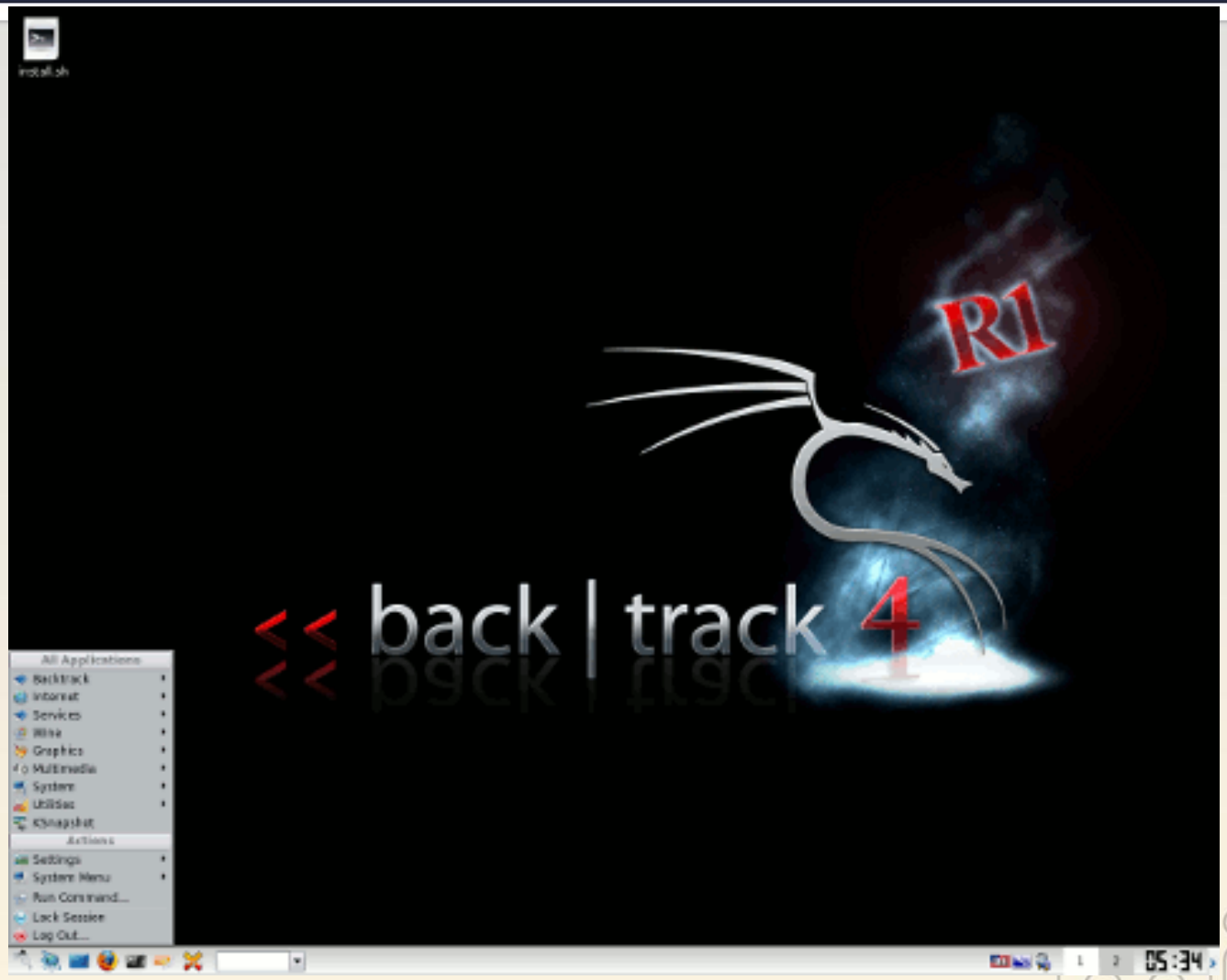
SuSE

VLOS

back|track

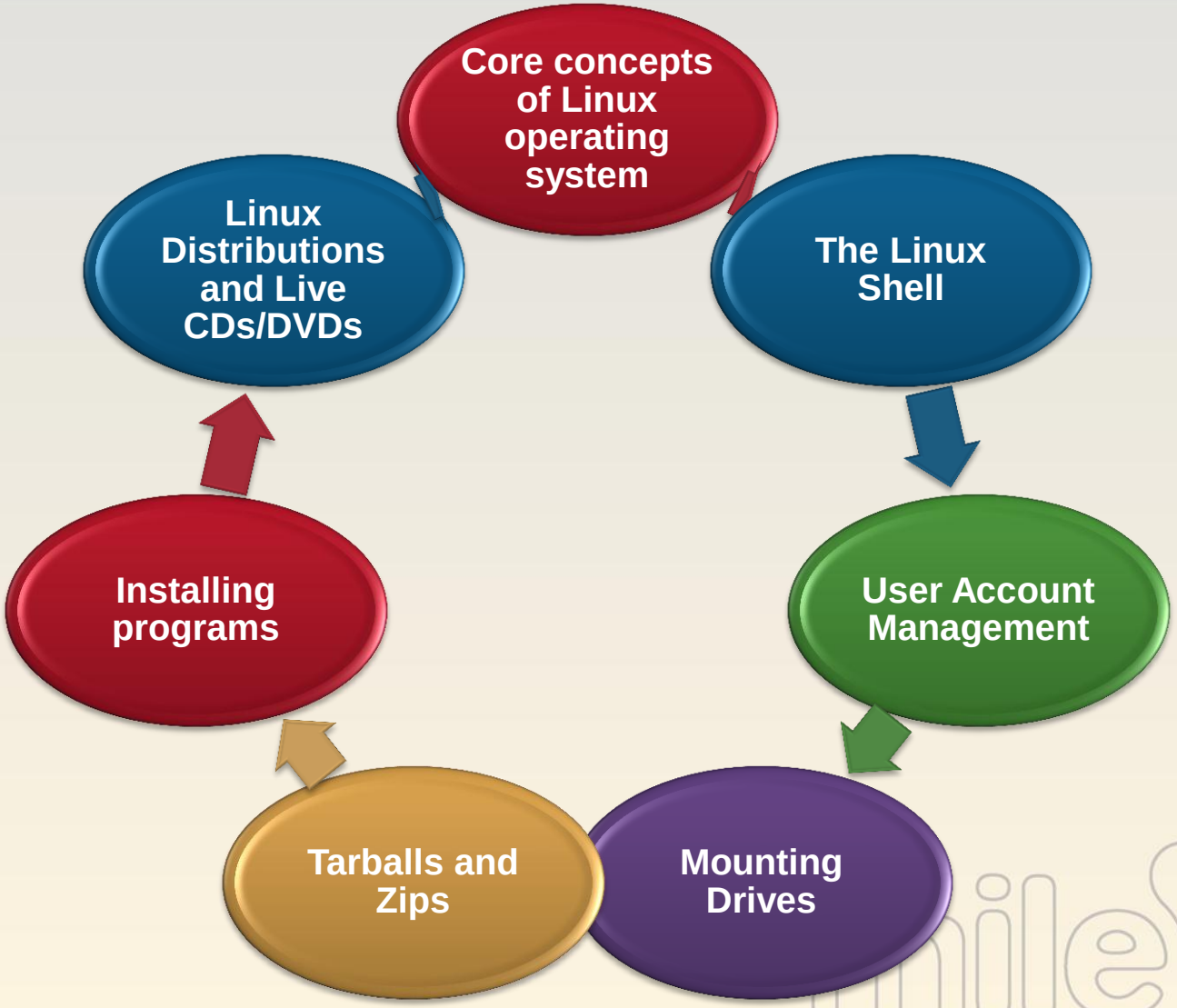
DistroWatch.com Put the fun back into computing. Use Linux, BSD.

Most Popular: BackTrack



http://www.backtrack-linux.org/

Review



Module 2 Lab
Linux Fundamentals