csc3412 Assignment 2

This assignment consists of 3 questions each of equal value. They consist of common tasks required of a system administrator—tasks I have had to do at some time in the past.

Clear Layout

It is vitally important that your assignment is clearly laid out with questions and parts of questions clearly defined. It must be a straight forward matter for the examiner to determine that you have completed each exercise satisfactorily. We want quality not quantity. Poorly organised submissions will be rejected or receive a poor mark.

A text file or PDF/A document typeset using vanilla LaTeX are preferred over a document produced by a word-processor. If you must use Microsoft Word please export your document as PDF/A[1] not PDF.

Command Output

When answering these questions you will have to run commands under Linux—whenever a command is run you will need to:

a. explain in your own words the purpose of the command in the context of the assignment question. (Please do not just copy the "Description" section from the man page!) Also, you need to explain in your own words all terminology used—as if you were explaining to an average user! (Please show you understand what you are doing!)

b. show that the command worked—either from its output or the output from another command. For example

```
prompt> dd if=/dev/zero of=Crypt.fs bs=1M count=32
32+0 records in
```

---

[1] PDF/A is an archival format of PDF that embeds all fonts used in the document within the PDF file. To ensure PDF/A format in Word check "ISO-19005-compliant (PDF/A)" under "Options" when saving a file as PDF.

```
32+0 records out
33554432 bytes (34 MB) copied, 0.109063 s, 308 MB/s

prompt> ls -l Crypt.fs
-rw-r--r-- 1 user user 33554432 2010-02-25 10:18 Crypt.fs
```

c. To capture text output from programs you will have to redirect the output to a file or use the command `script`. If you are using the command `script` turn off the tty escape sequences that change the colour of console text—the escape sequences will appear in output file and make it impossible to read.

Question 1 (marks 20)

The web administrator of your organisation needs to login remotely to the machine that is running the organisation's public web site.

You tell her that the only way to login is via The Secure Shell— which she knows nothing about! Assuming she is logging in via a Linux box write a help document for her containing the following—

a. (6 marks) A short introduction to SSH, explaining why it is the preferred way of logging into a remote machine—this explanation will need to discuss symmetric and asymmetric key encryption.

b. (7 marks) A discussion of the contents of the file `~/.ssh/known_hosts`.

   Your discussion should include (but not be limitted to):

   - how the file is populated,
   - how the keys in the file are used by SSH,
   - a discussion of "man-in-the-middle" attacks,
   - why the hostnames in the file are "hashed", and
   - how individual keys can be deleted by `ssh-keygen`.

c. (7 marks) A description how to configure access so that no passwords are needed—that is by using user asymmetric keys. This will require a discussion (with examples) of the command `ssh-keygen`, the file `~/.ssh/authorized_keys`, passphrase protected keys and the commands `ssh-agent` and `ssh-add`.

Notes:

a. Any technical term used must be explained.

b. Your virtual Debian has the SSH dæmon installed and running by default—so you can SSH to it from the host system or from a second virtual machine.

c. Your virtual machine has two network interfaces configured— a host only interface and a NAT interface. To bring the host only network "up" study the man pages `interfaces(5)`, `ifup(8)` and `ifdown(8)`.

d. You must show the relevant changes/parts of any files discussed.

e. This is a help document so you must explain (in your own words) the purpose of every file and command mentioned (plus any command line options).

f. Be very clear which key (public or private) is stored on which machine (remote or local)

g. Port forwarding, SSH tunnels and firewalls need not be discussed—they will be covered later in the course.

Question 2 (marks 20)

a. (8 marks) In about a page explain in your own words what a Logical Volume Manager is, its purpose and why it is useful.

b. (6 marks) Illustrate your explanation by using the Linux Logical Volume Manager to combine the two spare disks available on the Virtual Debian distribution. Combine the two disks into one logical volume. Format the new logical disk and modify the `/etc/fstab` file to mount the new disk at boot.

c. (6 marks) Document and explain in your own words the purpose of every command you use (plus any command line options) and any configuration files or scripts you modify or create.

Notes:

a. Be certain to explain the meaning of any tehnical terms you may use—for example, what is a "physical volume", a "volume group", &c.

b. Make use of the utilities `pvdisplay`, `vgdisplay`, &c. to show the results of commands and that they have worked.

Question 3 (marks 20)

A user comes to you requesting that you create and implement a backup policy for his desktop machine. What he wants, is to be able to place a blank DVD in his Single-Sided DVD-burner at the end of the working day on a Friday and have all the files he has been working on for the week backed up automatically that evening to the DVD!

After a bit more questioning you find out that:

- He frequently creates/deletes and changes files on a daily basis.

- He wants to be able to recover files for any given day.

- He only wants his home directory backed up.

- His home directory contains about 2Gbytes of data.

- His desktop machine has a spare disk (mounted as `/spare`) that has plenty of free space for temporary storage.

Tasks that need to be done:

a. (8 marks) Using the information above design a backup policy. Give a detailed description and justification of your backup-policy.

b. (8 marks) Using `tar`, a shell script or scripts and a crontab file implement your backup policy.

c. (4 marks) Document and explain in your own words the purpose of every command you use (plus any command line options) and any configuration files or scripts you modify or create.

Notes:

a. Use `/spare` as a temporary storage for backup files until they are burnt to the DVD on Friday.

b. "Temporary Storage" means just that—cleanup `/spare` after a *successful* burn.

c. A Single-sided DVD can only hold 4.2GiB $(4.2 \times 1024 \times 1024 \times 1024$ bytes) of data.

d. The ISO9660 file-system—is the file-system used on Optical disks.

e. To write data to an optical disk a complete ISO9660 disk image file containing the data, must be created on the local hard disk and then burnt to the optical disk.

f. You will need utilities for creating ISO9660 images and burning DVDs, have a look at the following packages `dvd+rw-tools`, `genisoimage`, `wodim`.

g. List all resources used in answering the question.