CAA3

General Observations

This assignment will be performed by working on the configuration files and commands available to configure and manage the corresponding services, avoiding as much as possible the use of automated tools and graphical user interfaces. These graphical tools can be used to verify the configuration and / or manage the application wherever possible, but not directly to solve the proposed exercises.

*Each question must specify **in detail** the steps taken and configuration changes performed, showing the results (wherever possible) through listings and other outputs **commented** by you and that may be reproduced so that they can be evaluated. Remember that assignments can only be assessed by the information contained in them.*

This assignment is an individual work. It will not be evaluated if parts of it are copied (from any source) or too similar to other students' assignments.

- (parts 1 and 2 were in the preceding assignment)

3. Set up a NFS server and a NIS server in the same machine. Both local and remote clients will connect via NIS and mount their HOME directories using NFS.
You must test the following features of the NFS server: restricted file access (e.g. read only), access limited to certain users, access limited to certain client machines.
The NIS system can be tested by configuring the client either in an external machine or on the same server. Note that testing client and server on the same machine requires creating NIS-only users and groups (i.e., that do not appear in /etc/passwd or /etc/group) and verify the connection in a terminal.

4. a) Install a mail service by configuring a MTA that can be accessed securely by IMAP4. Test the MTA locally and remotely. The service must include a junk mail (spam) filter.
b) Set up a web file server using WebDav. You must show that the service works by copying or moving files in the server and modifying their properties (access privileges).

5. Implement a firewall using iptables to allow access to Apache and SSH from a set of IP addresses. All other packets will be discarded (DROP)
Verify from a remote machine that the firewall works by scanning open ports with nmap or a similar tool. If you don't have access to another machine you can use a web service like GRC's ShieldsUP! [http://grc.com]. (keep in mind that many DSL routers already include a firewall that blocks incoming connections).
Your reply should include all the steps taken to configure the firewall, an explanation of every rule and the tests performed.

6. Taking the section on Security Administration as reference, do a full security analysis of your machine. You must analyse at least:

a) Whether there have been intrusion attempts. You must simulate at least one such attempt and describe how it can be detected.
b) The general status of local security
c) The general status of network security

The final report will include all the weak points found during the analysis or, if there are none, which possible weak points have been analysed to reach this conclusion.