Linux Installation and Configuration Self-Assessment

You have been provided with the following hardware:

An Intel-based PC with:

- Pentium-II 400 MHz Processor
- 128 MB SDRAM
- 4 GB EIDE Hard Drive
- 1.44 MB 3.5-inch Floppy Drive
- 40x EIDE CD-ROM Drive
- A 100-Mbit Internal PCI-based Ethernet Network Interface Card
- 15-inch Generic VGA-compatible Monitor
- 4 MB ATI Mach64 Type Video Graphics Adapter
- PS/2 101-Key Keyboard and PS/2 3-Button Mouse
- Standard Serial & Parallel Ports and 2 USB Ports

You also have been given a Red Hat Linux 8.0 CD Distribution (6 CDs Total – 3 Binary Install CDs, 2 Source Code CDs, and 1 Documentation CD), and five 3.5-inch 1.44 MB Floppy Disks (for whatever purposes you may think you need (creating boot floppies, rescue disks, backups, etc.).

You have up to 2.5 hours to install, setup and configure a functional and working Linux System to a set of certain specifications. The hardware you are given has no operating system nor software installed on it. The things you must try to accomplish in the allotted time are the following:

Complete a freshly-installed Red Hat Linux 8.0 System with the following parameters:

Your System Hostname: *bigserver1.example.com*

Filesystem	Size (MB)	Filesystem Type	RAID Level
/	1500	ext3	None
/boot	64	ext2	None
swap [1]	128	swap	None
/home [2]	1024	ext3	5
/data [3]	288	Reiserfs	1
/root	262	ext2	None
/junk	250	Reiserfs	None

Notes:
[1] **swap** must be made of two (2) separate 64 MB Partitions on the hard drive.
[2] The **/home** partition must support both User and Group Quotas.
[3] The **/data** and **/junk** partitions must allow any Student Account read/write access.

Create 100 (one hundred) Student Accounts, with the user name syntax of *studentX*, where *X* is a number from 1 to 100. For example, create Student Accounts for *student1, student2, student3* … and so on and so forth, all the way to … *student97, student98, student99, student100*.

Assign an initial password of *student* to each of the 100 Student Accounts. All Student Accounts must be set with an Expiration Date of June 15, 2003. Therefore, no Student Account should be active or usable after that date.

When any student changes their Student Account password, they must keep any password change they make for a minimum of 5 days before they are allowed to change their Student Account password again.

Configure the System so that each Student Account cannot contain more than 5 MB of data and/or files in their respective home directory (/home/*studentX*) – data and files owned by each respective user.

Configure the System so that Student Accounts 1 through 50 have *Bash* as their default shell, and Student Accounts 51 through 100 have *tcsh* as their default shell. Implement shell login time restrictions, so that users of the Student Accounts can only log in to the system between 8 AM and 5 PM, Monday through Friday – all other times should disallowed for logging-in.

Make sure that when each Student Account is created, that each Student Account home directory gets the standard new account directory structure, and a README text file that is 100 characters or less (the README file can contain any text).

Configure, build, and install a new modular 2.4-based kernel based on the Red Hat sources that has no support for IrDA and no support for ISDN, but does have support for read-write NTFS Windows filesystems, Ethernet networking, and all other services your server must support.

Create a boot floppy disk based upon the kernel and modules you built and installed.

Configure the System and/or the bootloader so it cannot make available nor boot the stock Red Hat kernel (the kernel that is installed during an installation). It must boot only the kernel you make/install above.

Configure the bootloader with a timeout value of 30 seconds, so it will boot a default kernel if no selection is made (and if additional kernels are installed later) by the user in that time. Also, configure the bootloader so it cannot be booted into single-user mode, unless a special password of *secret%boot67* is used. No password should be required to boot the System in its default configuration (Runlevel 3 – see below).

Configure your ethernet network interface so it has two bound IP addresses, and can see and communicate with two different subnets (all from one Ethernet card and cable plugged into your System). Here are the networking parameters to use for your eth0 interface card:

	eth0	**eth0:0**
IP Address:	192.168.20.1	192.168.30.1
Subnet Mask:	255.255.255.0	255.255.255.0
Gateway:	192.168.20.254	192.168.30.254
Nameserver:	192.168.20.254	

Configure and enable IP forwarding as a default setting for your System.

GNOME, KDE, and any X Window capabilities must <u>not</u> be on the System. All interactive usage with the System must be done only from Virtual Consoles. The System must boot by default into Runlevel 3 only.

Configure the System to only have 3 Virtual Consoles, specifically *tty1*, *tty2*, and *tty3*.

Configure the System so only the root account can log interactively (sitting down at the) System. All other accounts (i.e. Student Accounts) can use the System as the setup dictates, but not by allowing any non-root users to use the System interactively (sitting down at the console and keyboard). Network access, not direct access, can be allowed as deemed fit and necessary.

Configure the Apache Web Server to serve three different web sites, all hosted from your System, and from different directories (and having two sites serving the same content from one directory). Create a simple HTML page for each website that is served from the root folder of each hosted web directory.

Configure the Apache Web Server to deny any web requests from any host at *badcompany.com*, for any hosted or virtually hosted website. Apache should also be tuned to launch 5 child server web processes when the webserver is started or restarted, but never have more than 50 web processes at any one time.

The Apache Web Server must run on port 8080, and you must also configure *Tux*, a high-speed kernel-based Web Server to serve static content on port 80 from at least one of your hosted web sites.

Create a subdirectory with the name of *secure* below the root web directory of one of the hosted websites, and secure it using an *.htaccess* file, hence requiring a simple name and password when anyone tries to access that directory or any of its contents via a web browser.

Create and install a self-signed SSL certificate for one of the System websites, so that it can be accessed securely via the HTTPS protocol. The SSL certificate must not need or require a password upon web server starts or restarts.

Install and configure the package *webalizer* so it keeps simple (default) web statistics for at least one website served by the Apache Web Server. Once set up, webalizer must show its reporting web page with a web browser request of *http://localhost/usage*

Set up a printer and print spooler with either LPRng or CUPS, enable the appropriate daemons to start in the default booting Runlevel, and also be shared to Windows clients via Samba.

Configure the Samba Server to share both the /data (sharename "data") and the /junk (sharename "junk") directories for read-write access to Windows clients. The Samba Shares must be browseable. All Student Accounts must be able to read and write to these shares. The Samba Server must also appear in the *MYNET* workgroup, and allow encrypted authentication from Windows clients.

Configure the Samba Server so it is only accessible from the 192.168.20. network, and not accessible from the 192.168.30. network.

Configure the Samba Server to be a Master Browser of the local subnet(s).

Set up an anonymous FTP server for anyone accessing it from the 192.168.20. or 192.168.30. networks, from 8:00 AM to 11:00 PM daily. FTP access should not be allowed from any other networks.

Configure the FTP server so it allows any one person (identified by a unique IP address) up to 3 simultaneous connections, but no more.

Set up a Telnet server, allowing access only from clients in the 192.168.20. network, and for those clients, only from 8:00 AM to 5:00 PM daily, and 8:00 PM to 11:00 PM daily. All other networks should be denied Telnet services.

Configure a mail server to send and receive mail on SMTP port 25.

Set up the mail server so it is not an open relay, and does not accept incoming e-mail from un-resolvable domains. Tune the mail server so it will not handle and reject mail messages larger than 5,000,000 byes in size.

Configure the mail server so it masquerades all outgoing e-mail under the domain of *example.com* (not *bigserver1.example.com*).

Configure POP3 and IMAP access for clients on the 192.168.20. and 192.168.30. networks. All other networks should be denied POP3 and IMAP access.

Set up NFS Services, exporting the /data and /junk directories for read-only access to the 192.168.20. and 192.168.30. networks. All other networks should be denied NFS access.

Configure the System to not accept, forward, or output ICMP/IP packets.

Configure the System to use NAT and IP Masquerade all packets destined for foreign networks to the IP address of 192.168.20.254.

Install a caching-only nameserver on the System, and that uses the address of 192.168.20.254 as an upstream DNS resolver. Do not configure or use the *forward first* directive in /etc/named.conf.

Install the local e-mail reader of pine on the System, so any authorized user connecting to the System can check, send, and receive e-mail.

Create a cron job, that is installed by root, that creates a tar-gzipped archive of the entire /etc directory, and copies it to the /root directory once a week, Sunday mornings at 3:55 AM.

Configure a local timeserver for the 192.168.20. network, to only serve time to that network. The time server must get its master time from *time.easystreet.com*.

Configure a DHCP server to give out information to clients on the 192.168.20. network. IP addresses should also be in the network range of 192.168.20.100 to 192.168.20.200, give out a Class C subnet mask, the default gateway for the 192.168.20. network, as well as the nameserver IP number. The default lease time should be one day, with a maximum of two days.

Set up a proxy server to be a web proxy for web browser clients who wish to use it. The proxy server should be set up with access control lists to allow web requests to all domains, except any servers in the *badcompany.com* and *hacker.com* Internet domains.

Alter the existing *tmpwatch* script in /etc/cron.daily so that sweeps are made every five days, rather than 10 days.

Install and setup a (MySQL or Postgresql) database server for only two users (and root), *student1* and *student2*. The database system itself should handle the authentication requests, and provide a command-line prompt for simple INSERTs, UPDATEs, SELECTs, and DELETEs.

Install and make available the GCC C and C++ compilers for any accounts that have valid shell accounts to the system.

Install and set up basic NIS Serving capabilities, under the NIS Domain Name of *RHDOMAIN*. When setting up the server, also allow the configuration to provide for having a slave NIS Server with the name of *bigserver2.example.com*.