CS 309
Assignment 1

1 Introduction

Your first task is to install Linux on your system. We are going to use Fedora Linux, which is a recent branch of Red Hat Linux. There are several ways to do a Linux install, but we are going to take the easy path. In the lab there are several copies of the Fedora Core 1 install set which is also known as FC1. The install set is comprised of 3 CD's.
If you want to create your own install set of CD's the process is documented in the install set create documentation.
The install process is documented in there in the install docs.

CS 309
Assignment 2

This assignment is going to be postinstall housekeeping.

1. Password your GRUB bootloader and see if it works. You can leave it this way or not, its up to you. Also change some of the other parameters like the timeout so you can see how it works.

2. Boot your system into single user mode to be sure that you know how to do this.

3. Turn off unused services on your system. If you're not sure, don't change it, but you can certainly turn off sendmail, httpd, smb, snmpd, named, ntpd, vncserver, yp*, mysql and postgresql.

4. Insure that telnet and ftp are not running on your system but ssh must be. This means that you need to stop telnetd or ftpd from running via xinetd. Then you need to get sshd running using chkconfig and/or services. When you try to use ssh it will probably fail because you need to open port 22 in your iptables. Don't open it up for everything, just for 153.90.199.0/21 and maybe your home address.

5. Set up logging for your iptables and observe the traffic for a few days. You can turn it off by commenting out the rules and reinstalling your tables, but it is worthwhile to see what shows up in your logs.

6. Make sure that your iptables allow all local traffic to avoid problems with simple local operations.

7. Set up your TCP wrappers by creating a /etc/hosts.deny file that contains only *ALL:ALL*. Then create a hosts.allow that contains only *localhost:ALL*.

CS 309
Assignment 3

You are going to map the startup process for your system as followed by init. Given that the boot loader has selected a kernel and loaded it and the init process is processing /etc/inittab, show what happens as the boot up and initialization of the operating system progresses.

Specifically, give the name of each major configuration file accessed and what happens in general. i.e. don't give the details of error checking and all of the incidental files accessed, but tell me what configuration files are read and what they do, what processes are started and so on.

One good way to do this is as a diagram showing the progress of the boot-up process until control is given over to terminal control.

CS 309
Assignment 4

1. What does the following script do?

```
#! /bin/bash
[ $# -lt 1 ] && set -- .

find "$@" -type d -depth -print |
    while read dir
    do
[ `ls "$dir" | wc -l` -lt 1 ] || continue
echo >&2 "$0: removing empty directory: $dir"
rmdir "$dir" || exit $?
    done
exit 0
```

2. What does the following script do?

```
#!/bin/bash
STARTDIR="/"

echo "Script started at $(date +'%T on %D') \n
Searching through the following directories:\n"
```

```
set -- $STARTDIR

a=1
while (($# >= $a))
do
echo $'\t' $1 # display the directory pathname being searched
shift
done

# end of display output for the user.

find ${STARTDIR} -name core -type f -exec file {} \; |
awk -F: '/core file/ {print $1}' | xargs -t rm

# now tell the user that the script has completed
echo "Script completed at $(date +'%T on %D') \n"
```

3. Create a shell script that will output the network configuration information for your system including the IP address, DNS server, domain name and gateway address. This information is in several files or can be gotten from some commands.
4. Create a shell script that will execute a command in every home directory. For example, you give it the command "chmod 700 .bashrc" and it executes it in every home directory.
5. Create a shell script that will save the checksum of every file in /usr/bin and /usr/sbin. The cksum command will give you a 32-bit CRC checksum for a file as well as the number of bytes. You would normally dump the output from this script to a file so that you could compare results at a later time, so the output should include the filename and the checksum.

CS 309
Assignment 5

This assignment focuses on user administration tasks. You are going to be required to perform some simple tasks that you might normally do to directly support user accounts: creation, deletion, modification and configuration. The things below are to make sure that you try some interesting things, but you should be trying to find things to do that you might do if you had lots of machines and users to deal with.

1. Add a group to your system named cs409 with gid 1000. Use the groupadd command but check the group file to insure it works.

2. Use *useradd -D* to display the useradd defaults from /etc/default/useradd

3. Set the expiration date for accounts to May 15 using useradd and check to see if the file changed. Turn in a listing of this file.

4. Modify the login.defs file for your system. The minimum acceptable password length should be 8. Test it on a few passwords and see if it works.

5. Look at the files in /etc/skel. They are all *dot* files, so you have to use *ls -a* to see them. Add some things to the .bashrc file. For example, an alias for ls like this:

   alias ls='ls –color-tty' Add anything else you think you would like users to have in

   their basic bash configuration files. You might also want to change something in .bash_profile such as adding another path to the PATH environment variable. Why would you put a setting here rather than in the system-wide configuration files?

6. Add a .Xresource file to /etc/skel. It should contain something like this:

```
XTerm*background:       navy blue
XTerm*cursorColor:      red
XTerm*foreground:       wheat
```

7. Look at the system-wide configuration files, /etc/profile and /etc/bashrc. man bash and look at the INVOCATION and READLINE sections to help you understand things. What things get set in *profile*? How does /etc/bashrc get executed?

8. Add a couple of users with useradd and see if the home directories and mail files are created properly. Try things like picking a bad password. Also, try overriding password expirations and account expirations. What users did you create?

9. One of the users should be an account for you and with the uid and gid set to the same as they are on the EPS 254 systems. To find out what that is, log on and enter the *id* command.

10. As root, *su* to one of your newly created users. What is the difference between *su user* and *su -l user*.

11. Delete a couple of accounts and make sure that all traces are removed from the system. What does this entail checking?

12. Use usermod to modify the properties of a couple of users. What things did you modify.

13. Add a user gjh. Set the password to something reasonable and notify me by mail what it is. This will be the way I access your system. Your email should include a line of the form: your name, your system name, the password for gjh with commas

    between the terms. For example: Les Cranium, cs25999, TheSecret*is456!!

14. Set up the sudoers file on your system so that you can do some things from your own account without having to su to root. Set it up so that gjh has unlimited access to root commands.

15. Turn on quotas on your system and set quotas for your users.

CS 309
Assignment 6

There are two parts to this assignment. One part for you to do on your own system, and part to be done as a group. For the latter, use the following groups:

Group 1: Albers, Collins, Martin, Wilson
Group 2: Becker, Diefel, Pascoe
Group 3: Berg, Erickson, Pearson, Stevens
Group 4: Billman, Howard, Seltzer, West
Group 5: Braun, Jackson, Schmidt, Tucker
Group 6: Byxbe, Kirkpatrick, Sommers, Verdon

Group Questions Turn in a single report for the group listing all names and the percentage contribution by each member. The report should show the result that you selected for each question.

1. Create a bash (sh) alias that will use *ps* to list all processes with the processes sorted so that those using the largest amount of CPU time (first key) and memory space (second key) listed first.

2. Modify syslog.conf to send *local0* facility log entries with a priority of *less than warning* to */var/log/local0-minor* and all with priority of *warning or greater* to /var/log/local0-major. Use the *logger* command to test that it works.

3. Create a script and cron job that will test the files in /bin, /sbin and /usr/sbin to see if they have been modified in the last hour.

On your own do the following and turn in the descriptions, scripts and/or configuration files:

1. Create an alias that would identify processes running on your system that are older than some given input value in days. Note, an alias could begin with a script (or two) that you write and then finally an alias.
2. Create a script or alias that would give the process number(s) and user name (s) that is(are) currently using a file. Look at the *fuser* command.
3. Look in /var/log and identify the content of the following files:
   - boot.log
   - messages
   - rpmpkgs
4. Install *swatch* via rpm on your system and configure it to notify you of failed logins, su's and sudo's. It is possible that swatch won't install properly due to some missing Perl modules. See the attached description for the solution.
5. Use *at* or *batch* to execute a simple command. For example"
   echo "Time for class" — at 8:50

CS 309
Assignment 7

1. Write a description of what each line does in your fstab file.
2. Use the df command to determine how much space is being used from each partition. Try the m option also.
3. Use the du command to see how space is being used in /var.
4. Get a floppy disk and build an ext2 filesystem on it. Mount it at /mnt/floppy. Copy some files back and forth. Now use another floppy or the same one and put an msdos file system on it and perform the same operations (Check out the question below that uses the ext2 file system on the floppy). Use fdformat to perform a low level format on the floppy before doing anything else. You don't have to do this for a hard drive as the low-level formatting is done at the factory.
5. Set up your system to automount your CDROM and verify that it works.
6. Use fdisk to get the data on the partitions on your hard drive and describe what you see. If you had a new 20 GB hard drive and you wanted to partition it into three partitions of 4, 8 and 8 GB, what would you do. **Please don't do this on the hard drive on your system. Just describe it.**

7. Use debugfs to dump the information about one of your partitions. Dump the output to a file so that you can annotate indicating what your see from the superblock and from the first block group. Also, list the deleted files on one of your partitions and see what happens. Dump one of the deleted files to a file on your disk and see what it contains.

8. Use tune2fs on the floppy disk you created to set the maximum number of mounts between file checks to 10; set the volume label to something you like; and change the percentage of reserved blocks.

9. Using *dump*, dump a small directory to a file. Then delete a file from the directory. Using *restore*, recover the deleted file. This is most easily done you using the *-i* option to run recover. Remember that backup and recover can't depend on an existing file system, so full pathnames are needed for the files backed up and when extracting, it attempts to place the extracted files on the same path starting at the current working directory. If restore asks for a volume number, give it the number 1.

10. Export /home/gjh from your system so that it can be mounted only by the host malt.cs.montana.edu with read-write access and with the uid and gid set up to match the normal uid and gid of gjh on your system. Hint: after modifying exports, you will have to restart your nfs services. You can use *etc/init.d/nfs restart* or *service nfs restart*. You can also run *exportfs -a* which simply updates the exports table for nfs.

11. Set up autofs for your cdrom and floppy.

12. Set up smartd to monitor your harddrive. Also run smartctl with the -Ha options and report what you find out.

CS 309
Assignment 8

1. Set up orca as a CUPS printer on your system. Since you can't print directly due to security considerations, you will have to print through esus where the queue name is orca. orca is a Postscript printer.

CS 309
Assignment 9

1. Using tcpdump answer the following questions?

   (a) What types of packets arrive or leave my system in a 5 second period. Not every packet, just what types. Which of these can you not identify?

(b) What happens on the network if I ping another system?

(c) Suppose you have reason to believe that someone is trying to exploit your web server. Give a tcpdump command to help test this theory.

2. Using Ethereal, capture 10 seconds of udp traffic. Try some of the nice features of Ethereal, such as filtering post capture with the display filters and sorting the order. For example, you might capture some TCP traffic and try to solve problem 3 above with Ethereal.

   In the interest of your learning to do this on your own, the documentation for Ethereal is at http://www.ethereal.com/docs and it is quite complete.

3. Use traceroute to check out the route to a couple of places, like google.com. Also, check out stanford.edu. This is interesting because of the difference in response times. Why?

CS 309
Assignment 10

1. For this assignment, rebuild your kernel. You don't have to make any changes, simply configure and rebuild the kernel so that it will boot your system. When it rebuilds, it will name the kernel as a *custom* version, so you don't have to save your old version.

   You don't have to turn anything in for this, but I will eventually have you boot the new OS to see that it works.

CS 409
Assignment 11

1. Using nmap do a couple of different scan. For example -sT and -sO. Also, try nmap with the *-O* option, with *-sT -p 1024-60000*.

2. Open port 80 in your iptables and run nmap to see if it finds it. Don't forget to close it when you are all finished..

3. Have someone else scan your system with a simple *-sS* parameter.

4. Install portsentry and tripwire. The rpms are available at the usual sites.

5. Start portsentry if it is not already running (use *service portsentry status* to find out. Then run a portscan against your system from some other host. Check the */var/log/messages* file to make sure that it was detected. Also, look in the /etc/portsentry/portsentry file (probably) to see if that host is now blocked from your system. Try another scan to see what happens.

6. Now look in /var/log/messages again at the point where you made the initial attack. You should see a line like this:

```
Apr 14 07:53:35 malt portsentry[516]: attackalert: Host 153.90.199.78
has been blocked via dropped route using command:
"/sbin/iptables -I INPUT -s 153.90.199.78 -j DROP"
```

   What is this telling you? Execute *iptables -L* to see if this is true. The new rule will be at the top and will not be identical to the one shown in the messages file. In order to get the host unblocked, execute *service iptables restart* and delete the entries from the blocked file(s). Restart the portsentry service.

7. Now try a more sophisticated scan, such as an -sF, sX or sN and see if that is also detected. You will need to do this from another host or have someone do it for you. Again, when you are done, clean up iptables and your blocked hosts files as needed.

8. Finally, install tripwire and configure it. Make some changes and verify that it works.

CS 309
Assignment 12

Choose between one of the two final projects.

1. Install and configure sendmail with the following capabilities:
   (a) Set up at least two aliases.
   (b) Set up the Access database to demonstrate REJECT, DISCARD and 501 controls.
   (c) Set up your sendmail to allow you to masquerade as another mail domain and try sending some mail. You may need send among yourselves to get this to work. Don't abuse this!
   (d) Set up two local virtual domains and users associated with those domains. You are likely to have some trouble sending to these from outside systems without control of the DNS tables, but you can try.

2. Install and configure the Apache web server with the following capabilities:
   (a) Set up the server operate properly on your system at port 80.

(b) Set the Document Root to /usr/www.

(c) Set up a public and a private area. The public area allows access by everyone, the private area only from 153.90.199 addresses.

(d) Set up user home web pages to be at /home/*username*/www.

(e) Demonstrate the use of htaccess files to control access and to require authentication.
