Adapted from:
Linux Security HOW TO
Jerry Winegarden
Revised 9/25/00

Fourteen Steps in Linux Security

1. Install/Configure tcpwrappers (tcpd) - controls which systems can access which network services

   ### To install tcpwrappers

   - Choose it during "Custom" installation, or
   - rpm -Uvh tcpwrappers* (available from RedHat CD or RedHat mirrors)

   ### To configure tcpwrappers, edit two configuration files:

   - **/etc/hosts.allow** (specify which systems allowed to access network services on this machine)
   - **/etc/hosts.deny** (specify which systems are denied access to network services on this machine)
2. Configure which network services are started up on demand (e.g. telnetd, ftpd, lprd, sendmail)
   edit **/etc/inetd.conf**
   Comment out unneeded services to prevent their being used to break into your system
3. Stop unnecessary network service daemons from loading at system startup (/etc/rc.d/init.d, /etc/rc.d/rc.local, /etc/rc/rc*)
   to reduce the chances of an exploit being used
4. Watch for and install most recent system updates (especially security patches)
   - Subscribe to update and security alert announcement e-mail lists
   - Obtain and install security-related patches as soon as possible
5. Use good passwords - no accounts without password - no trivial passwords
6. Protect your passwords: use secure-shell **ssh** instead of telnet/ftp
   Never use telnet, rsh, rlogin, rcp over the Internet (unless absolutely necessary), because they expose your passwords in clear text. Use ssh instead.
7. Before starting a network service, first learn what it does and how to properly configure it.
8. install **pidentd** - helps log info about attempts to access your system
   to install: rpm -Uvh pidentd*

   - From http://www.redhat.com/swr/i386/pidentd-3.0.12-4.i386.html

9. Check system log file for curious messages, including access denies:
   /var/log/messages

10. Make **backups**: make a plan and use it - to let you recover from an attack more easily. Make an immediate backup first.

    Additional, but slightly more complex steps:

11. Run **Tripwire** to help detect security compromises.
    Find Tripwire:

    - http://www.tripwire.com

12. Install firewall - ip masquerade via ipchains
13. Read lots more about Linux security - this is only a start.
    For example: http://scrye.com/~kevin/lsh/Security-HOWTO.html
14. BE EVER VIGILANT - Security is a continual process

Note: these security steps should be taken immediately upon linux installation.

The details of each of the above steps is presented below.

How To Configure tcpwrappers: hosts.allow, hosts.deny

1. Change directory to /etc (cd /etc)
2. edit the files **/etc/hosts.deny, /etc/hosts.allow** (using a text editor, such as vi or pico).
   The files should look like:

File Name	File Contents	Explanation
/etc/**hosts.deny**	**ALL: ALL**	First, DENY ALL services to ALL systems.
/etc/**hosts.allow**	**ALL: LOCAL**	Now, specify which systems get allowed in. Extremely closed: no logins from any remote machine.
/etc/**hosts.allow**	**ALL: LOCAL, .duke.edu**	(Allow logins from any duke.edu machine. (Note the "dot" ahead of the duke.edu

		string)
/etc/**hosts.allow**	**ALL: LOCAL, 192.168.1., 192.168.5.6**	(Allow logins from any machine on subnet 192.168.1. (i.e. any 192.168.1.x where x=0-254. Note the "dot" at end of the string. Also allow logins from the machine with IP 192.168.5.6)

Explanation of syntax of entries in hosts.allow and deny

In /etc/hosts.deny and hosts.allow, certain keywords are allowed. ALL means just that: ALL services or ALL machines. LOCAL means the machine named "localhost", i.e., your own computer (you can log into your own computer: telnet localhost or telnet 127.0.0.1). Service names are listed to the left of the colon, while machines are listed to the right of the colon, specified by name or by number. Commas separate items in the list.

In /etc/hosts.deny above, the first ALL refers to ALL **services.** The second ALL refers to ALL **systems.** Services, such as telnet or ftp or http can be listed separately, with a different allow or deny list for each one. Machines or subnets can also be specified by IP number in deny or allow. For example:

ALL: LOCAL, a.b.c.d, e.f.g.

would allow (or deny) access to all services by the machine with IP number a.b.c.d, and to all machines on the subnet x.y.z (note the "dot" after the the last number represented here by z), for example, x.y.z.1, x.y.z..2, etc.

See **man hosts.deny** or hosts.allow for examples. If there are specific machines outside of Duke to allow access from, then add them explicitly to the hosts.allow file. Remember, when you go home for break, you need to consider this configuration if you want to access your machine at Duke from a machine at home.

How to configure /etc/inetd.conf

Comment out every line in this file (by placing a # sign at beginning of line) **EXCEPT** the following lines:

```
auth  stream tcp wait root  /usr/sbin/in.identd in.identd -e -o
ftp   stream  tcp  nowait  root   /usr/sbin/tcpd  in.ftpd -l -a
telnet stream tcp  nowait  root   /usr/sbin/tcpd  in.telnetd
```

The lines ftp and telnet lines you may consider leaving (if you need remote access to your box from other machines via telnet or ftp for home). Once you get ssh/sshd, you may

want to comment out the telnet and ftp lines in /etc/inetd.conf and add a line for sshd. Then you could only get to your box via ssh, not via telnet or ftp. However, if access is required from a machine out on the Internet and it does not have ssh installed, then you need to leave telnetd and ftpd in inetd.conf without comment (#), or uncomment them if you've disabled access via telnet or ftp. (Note: the service process's name for telnet is telnetd and for ftp is ftpd.)

(Note: if an entry in inetd.conf is listed as:

```
telnet stream ...  /usr/sbin/tcpd  in.telnetd
                           ^^^^     ^^^^^^^
```

then it is started up by the **tcpwrappers** daemon, **tcpd**. If a process is started by tcpd, then it pays attention to the /etc/hosts.allow and deny files. If your system does NOT have /usr/sbin/tcpd, then you do NOT have tcpwrappers installed. You need to install it as soon as possible.

Stopping unnecessary services from starting up on your system

When your system starts up (into run levels 3 or 5), several services are started up automatically. If the service's daemon is listed in: /etc/rc.d/init.d then it probably starts up. These services, such as tcp/ip can be stopped and started under Linux (System V method) manually using the syntax: /etc/rc.d/init.d/lpd stop (or start or restart) where lpd is the name of a daemon in /etc/rc.d/init.d (lpd is the print service daemon). The easiest way to change what will start and stop automatically upon system boot is to use **linuxconf**. Installing a network services package will usually configure the system to start it automatically. Starting a web server or mail server or name server without editing the config files for security can be an open invitation to be cracked. Learn first. If you don't know how, ask!

Change what services will start automatically at system boot

How to use linuxconf to make these changes

Start linuxconf from a regular shell "terminal" window (command line prompt):
linuxconf &

(In following discussion, ==> means **"click on"**
E.g. aaa==>bbb==>ccc means
"run aaa, then click on bbb, then click on ccc,...")

linuxconf==>Control==>Control Panel==>Control service activity

(linuxconf "Service control" window pops open)

The table of services will look like:

```
Name                    Enabled         Running

apmd                    Automatic       Running
arpwatch                Manual
atd                     Automatic       Running
bootparamd              Manual
crond                   Automatic       Running
dhcpd                   Manual
firewall                Manual
gated                   Manual
gpm                     Automatic       Running
httpd                   Manual
identd                  Automatic       Running
inet                    Automatic       Running
keytable                Automatic       Running
kudzu                   Automatic       Running
linuxconf               Automatic
lpd                     Automatic       Running
mars-nwe                Manual
mcserv                  Manual
named                   Manual
netfs                   Automatic       Running
network                 Automatic       Running
nfs                     Manual
nfslock                 Manual
nscd                    Manual
pcmcia                  Automatic               (if laptop, Running)
portmap                 Manual
postgresql              Manual
random                  Automatic       Running
routed                  Manual
rstatd                  Manual
rusersd                 Manual
rwhod                   Manual
sendmail                Manual
smb                     Manual
squid                   Manual
syslog                  Automatic       Running
xfs                     Automatic       Running
xntpd                   Manual
```

In general, you should start with only the above services listed as "Automatic". You may want to add something (e.g. if you want to receive email on your box (and not just ssh to godzilla for pine).

To change the status of a service, DOUBLE CLICK the name.

==>sendmail

("Service sendmail" window pops open.)

```
"You can enable/disable a service
or you can start and stop it manually"

Startup         Automatic      (click to select or unselect Automatic)

Status
Description     Sendmail is a Mail Transport Agent, which is the program
                that moves mail from one machine to another.

Package name    (No package manager available)

Choice of buttons:

Accept  Cancel  Start  Stop  Restart  Help
```

Start, **Stop**, **Restart** manually change what is running now.
Cancel quits out of this window.
Accept accepts the changes you have specified (for automatic startup).
Note: the changes specified using linuxconf are not actually implemented until the "**Activate Changes**" command in linuxconf, which is what to do next.
Note: "Quit", which will prompt for "Activate Changes?" before it quits linuxconf)

==>**Accept** (closes "Service Sendmail" window, opens "Service control" window.)

==>**Quit**

==>**Act/Changes** (button)

"Status of the system"
The state of the system is not in sync with the current/updated configuration. You are allowed to make it current, or continue with the current configuration. You can also look at the things that will have to be done to make the system current.

```
==>Activate the changes
   Preview what has to be done

If there are problems, you will get the error message window:

"There were some errors"

Some errors were reported
Do you want to examine the logs

Yes  No
```

If there are problems, you may not have configured the service properly. Suggest you quit and ask for help, if you don't know how to troubleshoot the service you just changed. If there are no problems, then you can just

```
==>Quit   Quit linuxconf.
```

chkconfig - Red Hat tool to configure which services are running

chkconfig is Red Hat's tool to configure which services (network and other) are running on a system. chkconfig is an alternative to linuxconf for configuring network services.

Subscribe to and watch for messages from RedHat Update and Security Alert announcement e-mail lists

For subscription information: Red Hat support lists. Obtain and install the relevant updates as soon as possible to close the newly found security holes. Note that not every update will apply, since you may not have installed everything.

Watch for messages with Subject line of: **[RHEA xxxx]** or **[RHSA xxxx]**
RHEA = Red Hat Enhancement Announcement - Update Announcement for a Red Hat package (from redhat-announce@redhat.com)
RHSA = Red Hat Security Alert - security alert, patch availability announcement (from redhat-watch@redhat.com)

Obtain and install updates and patches as soon as possible

If you are alerted to the existence of updates, check out the redhat errata pages, or go to a mirror site such as: ftp://metalab.unc.edu/pub/linux/distributions/redhat

Check out the list of Red Hat Linux resources for additional sites to look for updates:

Red Hat support list
Linux support resources list

Use Good Passwords

Choose good passwords. Don't allow trivial passwords such as: password, pass, username, initials. Another suggestion is to mix letters and numbers and symbols. Make at least one substitution of a number or symbol such as ! in place of a letter. This makes it (slightly) harder for password-guessing programs that have dictionaries to guess a password for an account on your system and thus to get in.

ssh: Protect your passwords: how to obtain, install, configure secure-shell ssh

Programs such as telnet and ftp send out "plain text" passwords. One solution to prevent your password being stolen on the Internet is to **use ssh instead of telnet** to remotely log into other systems. The requirement is that the remote system that you want to log into must be running the other half of ssh: sshd, the daemon that listens for and establishes ssh logins. At Duke, you must use ssh to log into the acpub machines, so it is a very good idea to install it. (Note: ssh uses "strong" encryption, which is still subject to some export restrictions by the U.S. government.) ssh is available on the Internet. We highly recommend it be used in the case where the machines you want to access are running it.

Learn How to Configure Network Services BEFORE You Start Them

It is important to learn how to properly configure a network service such as a web server (httpd=apache web server), or ftp server. Improperly configured services can be an opportunity to be successfully attacked by intruders

Install pidentd - helps log attempts at system access via network

To install: rpm -Uvh pidentd* (from the Red Hat CD or from the mirror sites). Look in the RPMS directory: **.../RedHat/RPMS**

Check system log file /var/log/messages

Commands to view system message file:

- **more /var/log/messages**
  (this may be a very large file to get to the end)
- **tail -n xxx /var/log/messages**
  Displays "tail" - last xxx lines of file /var/log/messages

Look for messages about "denied" access. Any time a system is denied access by tcpwrappers (hosts.allow,hosts.deny), the incident is logged in /var/log/messages. Look to see what systems are trying to access your system. In some cases, this information can be used to stop attacks. If you do get such messages, check out:

More Advanced Security Steps

Install Tripwire

Tripwire is a package that can help you lock your system up tighter. As the name sounds, it is intended to be a "trip wire" in case someone does break in. That is, if someone breaks in, it's supposed to notice before the vandal has a chance to cover his tracks. Some network access is quite valid. Other attempts at access may be for hostile purposes. Tripwire can help detect security compromises.

Find Tripwire:

- located on RH Apps CD
- the Catalyst CD from www.lsl.com
- http://www.tripwire.com

Learn More About Linux Security

- subscribe to linux security e-mail listserve: mail -s subscribe linux-security-request@redhat.com < /dev/null
  (Actually, send subscription message from machine that will use to read email).
- Regularly read the Linux security web pages: http://www.aoy.com/Linux/Security
- Read other Security documents. For example:
  http://scrye.com/~kevin/lsh/Security-HOWTO.html

Be ever vigilant

Don't stop watching your system for break-ins. Don't stop looking for ways to improve security. It is a never ending process just as with "Spy vs Spy" (the old Mad Magazine feature).