Appendix H

Steps for securing Linux

With the rapid expansion of today's Internet, more and more machines have become targets for hackers. Due to the LearnCanada requirement and certain limitations on the applications being used, it was requested that all sites be situated in front of their network firewall. Once these workstations were up and running, they become likely targets for hackers, if certain pre-cautions are not taken. Although securing a site is a very large task itself, taking basic measures preventing any type of hacks is necessary. The following section will outline the minimum requirements, which each site was asked to take to secure their machines and network.

(i) Patch updates:

Updated patches are essential. Redhat continuously release security alerts as they become known. Patches for this alerts are readily available. Simply update the rpms to the most current patches is one way to stay ahead in the game. Installation of the patches are simply done as an RPM upgrade. The bash command for upgrading is "rpm -Fvh <filename.rpm>". The latter versions of Redhat has an automatic update software, similar to the Windows based applications.

(ii) Open ports.

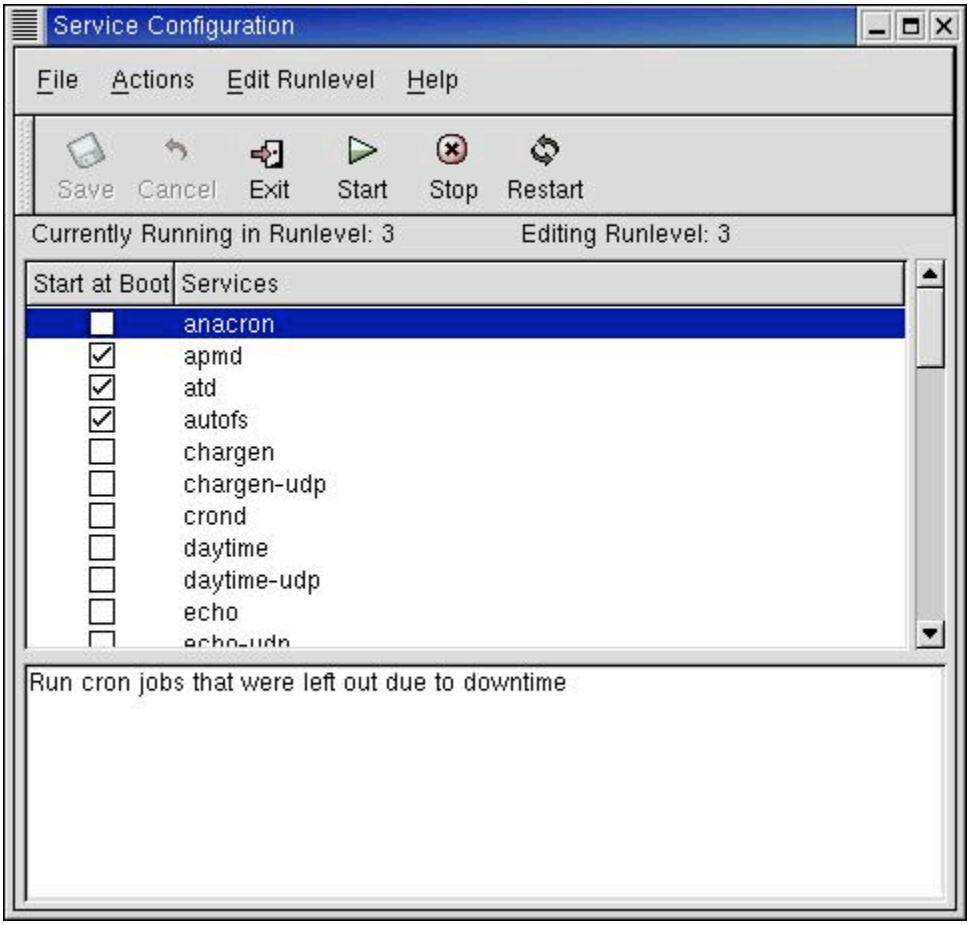
In a default installation, Redhat Linux will install various demons in the startup script. Many of these demons are not needed for the LearnCanada project. It was advised that all sites shut down all unused ports like, sendmail, portmap, wu-ftp, etc.

Open Ports:

To see what ports are open, the following bash command can be run from the terminal window. "netstat -antup". The following is an example resulting from the command.

```
# netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q  Local Address      Foreign Address    State       PID/Program name
 tcp    0      0     127.0.0.1:32768    0.0.0.0:*          LISTEN      989/xinetd
 tcp    0      0     0.0.0.0:6000       0.0.0.0.*          LISTEN      -
 tcp    0      0     0.0.0.0:32769      0.0.0.0:*          LISTEN      789/rpc.statd
 tcp    0      0     0.0.0.0:111        0.0.0.0:*          LISTEN      761/portmap
 tcp    0      0     0.0.0.0:22         0.0.0.0:*          LISTEN      956/sshd
 tcp    0      0     127.0.0.1:25       0.0.0.0:*          LISTEN      1364/sendmail: acce
 udp    0      0     0.0.0.0:32771      0.0.0.0:*                      789/rpc.statd
 udp    0      0     0.0.0.0:111        0.0.0.0:*                      761/portmap
```

As you can see, many unnecessary ports are open for potential hackers. To disable the ports permanently, you can run "serviceconf" in the terminal window.



Disable all ports not necessary or are considered potential security risks. Eg; sendmail, portmap, nfs, xinetd, talk, lpd, are not normally needed in for this project.

Once these are all shut down, you will notice that port 6000 will still remain open. This is the Xserver port. This may be shutdown if you are do not plan to run a separate display monitor. To shut this port down, the following command must be added to either one or two files, depending on the runlevel you are running.

To determine which run level you are running, run "cat /etc/inittab | grep id". If the id is 5 your are running runlevel 5 and the command ling

If the id is 3, the command line [serverargs="-notcp listen"] must be added to the /usr/X11R6/bin/startx file.

(iii) IPChains and/or IPTables.

Simply put, IPChains or IPTables is a Linux Firewall. It was mentioned above that all LearnCanada site networks must be situated in front of their network school boards firewall. However, this firewall only opens specific ports needed for the ISABEL applications and other services. All other ports will be blocked.

Specific ports can be set on the ISABEL application to allow transfer of packets. However, default ports can be used. The default ports which must be open for the ISABEL application is ports 32000 to 32008 for UDP packets. As well as ports 12344 and 12345 for the TCP packets.