SECURING YOUR NEW LINUX BOX

You've finally done it, you have thumbed your nose at the monopoly which is Microsoft, you have installed linux. Well done! Glory in that newfound feeling of freedom! Unfortunately I have to interject with some harsh realities though, you still have work to do. Even with linux, you have to go that little bit further to make it more secure. But fear not, it is not difficult, in fact here is a general list to work through, just remember - "That which is not explicitly permitted is expressly forbidden"..

- *Patch and Upgrade*
  You must always make sure that you are using the most secure versions of the kernel and software on your machine. Be aware that the main benefit of open source is that any program has many people checking it out. If something wrong is found then -more often than not- a patch or new version is released to fix the problem. Make sure the software you are running has no problems, you may even consider running a vulnerability scanner against your machine to double check it.

- *Remove Unnecessary User Accounts*
  There could well be users and groups which are installed by default, and many of these are never used. These unused accounts or very often used by attackers. Disable them first to see if you need them, that way if critical software stops working you can enable them again. However if your machine functions fine without them, then remove them totally. If you have multiple users on your machine the same rule applies, you must make sure there are no old accounts active. If you see a user account you are'nt sure of if it is used or not, try "*find / -user <user_name> -print*", this will give you list of all files owned by the specified user. If the files are minimal and/or very old, the chances are that it is safe to delete the user.

- *Change Banners*
  Most versions of server software show a system banner when a client connects. These banners very often give away important details which can be useful to attackers. Make sure that you do not allow these banners to display. If you feel very sneaky you could even change the banners to give false information, you know, just to throw a bit of a false scent.

- *Increase Logging*
  Make sure that all logging activity is recorded, and that it is of a detail which you find useful. Also think about using an automatic log filtering program to help you track and read the logs. Another handy trick is to configure logging to another system, this allows for both safer logs and centralized viewing of the logs. Remember logs are the history of your machine, keep them safe.

- *Disable CTL+ALT+DEL*
  Many linux systems recognize this "three finger salute" as a shutdown command. This is very bad as anyone who has physical access to the server can reboot it without knowing any passwords. Change this in the runlevel file (normally /etc/inittab). This does not take the need for physical security, it just removes another way the system could be attacked, or even accidentally shutdown.

- *Remove Unneeded Applications*
  Your system should only have the software on it that it needs to perform its business functions. Leaving other software running or even on the server can often leave more ways an attacker can compromise your system, but if nothing else, it gives them more files to hide amongst. Be especially cautious of compilers and network diagnostic tools. Use your package management system to remove unneeded software as a first step, and then start weeding it out manually. If in doubt man pages, package information and even the web can tell you what a certain app or file is used for.

- *Disable Unused Services*
  Many default installs have some default network services running. Turn off all the ones you do not need (xinetd, inetd, rc runlevels, etc). Doing this not only reduces the possible entry points an attacker can use, but also reduces the system administration overhead as you can concentrate on monitoring only the needed

services. You can run a port scanner against your machine to check for running services. Checking for unused services is also not something you do once but periodically to ensure your system is secure.

- *Enable IPTABLES*
  Even if you are running a simple server you can and should enable and configure IPTables, the inbuilt linux firewall. Even if the machine does sit behind a normal firewall, having a firewall running on your host helps enforce proper network usage. This is an implementation of the "defense in Depth" principle, where you make an attacker fight for every bit of access he wants.

- *Use Sudo*
  Full and blanket usage of the root account for day to day working with your server is a bad thing, especially if you have multiple people working on the server, each undertaking some administrative functions. It is much better to rather create sudo entries for each task the various administrators need to perform so that there is less risk of major disasters when something goes wrong. It also increases the accountability each administrator will have for their actions on the server.

- *Use CHROOT*
  Using CHROOT restricts a given service or user to an isolated area of the system, which means that even if the service is compromised then the damage is limited to just the isolated area rather then compromising the entire server. This is useful because while some servers are inherently insecure you will be forced to run them (business requirements, because the customer says so, etc), this measure can limit the damage any compromise can do.

- *Check Files*
  Install some type of measure which can monitor important files and notify you of any changes which may occur to these files. Doing so will help you keep track of what is happening on your machine, and also what files you can and cannot trust. These logs are also useful in helping rebuilt the system, as if you have some idea of the extent of the attack you will better be able to choose to rebuild or reinstall.

- *Limit Suid File Usage*
  Leaving files lying around your system that have the superuser privilege bit set, can be an easy way in for an attacker. Take a bit of time to identify these files, and if they do not need to suid bit set then remove it. Another option you have is to set the suid bit to run as a user with lesser privileges as this will also lessen the damage exploiting this files can cause.

- *Install An IDS*
  Install an Intrusion Detection System to help you monitor what is happening to your box, and to help you track and monitor any unwanted or suspicious network traffic so you can decide if you should take further action or not. Remember the more you know about what happens to your machine, the better you can protect it.

Well I hope that helps, but bear in mind this is a general list. There are times when you might not be able to implement some of these or when you may need to implement more stringent measures, but whatever the circumstances this list should be a good start towards a secure linux machine.