

*Nix Distribution Rebuild Guidelines

These are self-help guides offered by the SOS office related to assisting you in reformatting your hard drive and reinstalling your operating system. Note: Anyone from outside The Pennsylvania State University network may not be able to view some of these files.

The documents on this web page contain only suggested guidelines for rebuilding and securing your machines. Because the process is different for every computer manufacturer, these guides are written at a high level. Any questions you have about this process should be directed to the [Help Desk](#), area [RESCOM](#), a faculty/staff IT contact or [Information Systems Consulting Services](#) for a specialized affordable alternative. Carefully consider which guidelines to implement, as every environment will have very differing needs and requirements. It is recommended that you implement one modification at a time to determine the impact of the change. Always be sure to document all modifications that are made and implement them in a test environment prior to deployment in a production environment.

While the *nix platform is not generally vulnerable to viruses and spyware due to the design of the operating system. You should always be aware of viruses. If you are serving files in any way to Windows clients, you should definitely be scanning for viruses. We do recommend the use of robust firewalls for preventing intrusions as well as using good administrative practices like not running applications and processes unnecessarily as the root user. Also view external resources <http://helpdesk.psu.edu/linux/spywrvirus.html> .

1. Disconnect from the network

Unplug the network cable and remove any wireless network adapters if you are near a wireless access point that allows automatic connections without any configuration by the user. If the wireless adapter is built-in, you are most likely using a laptop. Take the PC somewhere out of range of the wireless network.

2. Back up your files

Consider the files that you need to keep (word documents you have written, school projects, e-mail). Make copies of the files that are unique to you or irreplaceable. You can use an actual back up program, or you can manually copy the files. Either way, you will need to get the files to a location other than the drive where you plan to install OS. Some examples, are; another hard drive installed in the PC or connected to it via cross-over, cable USB or FireWire, one or more CDs or DVDs, another computer, via the network, zip disks, Jaz disks, or SuperDrive. Do *not* include any system files in the backup, and system configuration files like `inetd.conf`. Limit the backup to personal data files only! You don't want to backup, then restore something that might open a backdoor or another hole.

3. Preparation Steps

Once you have reformatted the machine, you will need to install several files before placing it on the network for the first time to prevent it from becoming infected again. Service Packs, patches, and hotfixes are software update programs which eliminate specific vulnerabilities that have been discovered in a larger piece of software. You will need to use either a writeable optical drive (CD/DVD-R), a mobile/external drive, a logical drive, or your [PASS](#) space (although PASS is limited in size) to download the updates and burn them to a CD **before** you do the reformat from another computer. Patches should be downloaded from a trusted machine rather than a compromised host. Apply all of the patches for your system level from your *nix distribution web site. For example Red Hat maintains an [errata page](#) listing current security patches for each of its systems. Continue to do this on a regular basis.

4. Reformat & Reinstall

Re-install from scratch using your *nix distribution CD, and reformat the drive during the installation to make sure no remnants are hiding. Replacing the drive is not a bad idea if you want to keep the compromised data available for further analysis. At this time, any rootkit cleanup tools that may be available on-line should not be used. They will not remove additional files/tools that were added after compromise/toolkit installation through remote control of the system.

Reformatting your machine removes all data from your computer. This is an irreversible process.

5. Create Passwords

Intruders do attempt to gain access to shared computer systems through the accounts of others. Their motives vary from curiosity to criminal malice. It is part of your responsibility as a computer user to create a strong password for both your Penn State access account and all operating system accounts on your computer. It is your privacy, your reputation, your files, and your computing resources that are all at risk. Often times passwords/password files are commonly collected for future use when a system is compromised. All passwords should be changed and strengthened in the event of compromise For detailed instructions on how to create a good password go to the [SOS passwords page](#).

6. Install Firewalls

It is important to ensure your firewall is enabled for complete protection. Be sure to disable unnecessary services (i.e. send mail, inetd, xinetd). Some general information and guidelines on firewalls can be found at the Penn State ITS Helpdesk links below. Most *nix distributions have firewall/filtering functionality included (e.g. ipchains, iptables, ipfilter, etc.) or that can be downloaded and installed. Also consider using *integrity checkers.

Unix/Linux	http://helpdesk.psu.edu/linux/sysseclinux.html
Tripwire (Intrusion Detection System)	http://www.tripewire.org
AIDE (Advanced Intrusion Detection Environment)	http://www.cs.tut.fi/~rammer/aide.html
chkrootkit	http://www.chkrootkit.org/

7. Automate Security Updates

New vulnerabilities are continuously discovered and attacks to exploit vulnerabilities are continuously written. Toolkits for installation once a vulnerability is exploited are also constantly being updated/created to increase their potential for disruption/destruction and make them more difficult to detect. Configuring your system to update security patches/virus definitions automatically with the directions below will help keep your computer protected. However, some updates are not able to automate so you need to continue to check the security pages frequently

Antivirus for Unix/Linux	http://helpdesk.psu.edu/linux/spywrvirus.html
Redhat Security Updates	http://www.redhat.com/security/updates/

8. External Security Guides and Documents

Unix Configuration Guidelines:	http://www.cert.org/tech_tips/unix_configuration_guidelines.html
Unix Security Checklist v2.0	http://www.cert.org/tech_tips/usc20_full.html
Securing your Linux desktop system	http://www.princeton.edu/~psg/unix/linux/linuxsecurity.html
Best Practices guide for securing the Linux Workstation	http://www.linuxsecurity.com/feature_stories/feature_story-115.html
Armoring Linux	http://www.spitzner.net/linux.html

Keeping Red Hat Linux Systems Secure with up2date:	http://www.sans.org/rr/whitepapers/sysadmin/1197.php
Unix System Management and Security: Differences between Linux, Solaris, AIX and HP-UX	http://www.sans.org/rr/whitepapers/unix/936.php
System Administrator - Security Best Practices	http://www.sans.org/rr/whitepapers/bestprac/657.php
Firewalling	http://www.seifried.org/lasg/firewall/
Unix Security Resources from the Advanced Laboratory Workstation System National Institutes of Health Center for Information Technology	http://www.alw.nih.gov/Security/security.html