Basic Security

These are things that every user can do to improve system security. Advanced topics will not be presented here, just the basics that every user can implement easily and will provide decent protection.

Use Strong Passwords

The strength of your password depends on three things:

1. Length: A longer password is a stronger password. Guides suggest at least 8 characters.
2. Complexity: The more varied the characters in the password, the stronger the password.
3. Deducibility: The harder it is for an attacker to derive a password the better.

Make sure to change your password often so that if someone is trying to crack it, they will have to start over. Also see the ultimate guide for creating strong passwords.

Disable Unused Services

On Slackware, make unexecutable any rc files in `/etc/rc.d` that start services which you do not use. For example:

```
chmod a-x /etc/rc.d/rc.gpm-sample
```

The less services you use, the less chances that one has a bug that will allow an attacker to exploit it remotely.

Setup a Firewall

On Slackware, the easiest way to do this is by using Alien Bob's adaptation of the Easy Firewall Generator. Just generate the firewall, copy the output to `/etc/rc.d/rc.firewall`, and make it executable.

```
chmod a+x /etc/rc.d/rc.firewall
```

Other options include GUI firewall generation programs such as Firewall Builder.

X -nolisten tcp

By default, the Xorg server listens to port 6000 for remote connections. Sometimes you want remote connections, but if you don't, then disabling it is a good idea. The easiest way to do this is by creating this file at `~/.xserverrc` **OR** `/etc/X11/xinit/xserverrc`.

xserverrc

```
#!/bin/sh

exec /usr/bin/X -nolisten tcp
```

You can specify more options to X in the same file if you need to.xserverrc

On Slackware, listening for incoming XDMCP requests is disabled by default in both xdm and kdm, so it is secure by default. One may ask, why bother stopping Xorg from listening if this is the case. It is always better not to trust config files, as exemplified by an old bug report when xdm ignored its config file.

Check for open ports

Some ways to check for open ports are:

```
nmap localhost
nmap YOUR_EXTERNAL_IP_ADDRESS
netstat -luntp
```

Your external IP address can be found at sites like http://whatismyipaddress.com/. If you don't know what a port is used for check the wiki.

Scan the system for malware

The following programs are useful for detecting rootkits and viruses:

- rkhunter
- ClamAV

Although not that much malware exists for Linux, it is a good idea to scan once in a while.

Sources

- the ultimate guide for creating strong passwords
- http://slackwiki.com/Basic_Security_Fixes
- http://slackwiki.com/Security_Assessment_using_Nmap

security, software, author htexmexh