



IF IT'S TECHNOLOGY
IT'S HERE.

Friday, March 28, 2014

Select Language ▼



| [Electronics](#) | [Solar](#) | [Consumer Electronics](#) | [Infotech](#) | [Linux & Open Source](#) | [Smartphones](#) | [Tablets](#) | [MWC 2014](#) |

EFY Expo 2014

Search



[Home](#) >> [Linux & Open Source](#) >> [Technology](#)

58 Cool Linux Hacks!


Efytimes brings to you 58 super cool hacks for all levels of Linux users!

Free Classifieds
SELL ANYTHING 

Sell Your Old Mobile at Good Price



POST A FREE AD

 **SmartMusafir**
Search Lowest Air Fares
On All Travel Sites
With One Click &
Earn Money
Everytime You Buy Airtickets

- **Linux Operating System**
- **Linux Server**
- **Computer Security Systems**
- **Wep Cracker**
- **Webcam Driver**
- **Downloads**

ads

Free Classifieds
SELL ANYTHING 

Sell Your Used Items



POST A FREE AD

SUBSCRIBE TO EFYTİMES
Receive the latest reviews, how-tos, news & more.

Enter your email address:

Are you ready to try your hands on these cool Linux hacks! Set your machine on and get started!

Subscribe

Delivered by [FeedBurner](#)

Most popular

Daily

Weekly

- » [The Best 20 Open Source Security Apps To Protect Your System And More!](#)
- » [10 Amazing Open Source Tools To Make Life Easier For Web Designers!](#)
- » [Love Open Source? Try These 10 Cool Apps!](#)
- » [Nokia's Android Phone, Nokia X, Gets Price Cut In India](#)
- » [10 Of The Best Open Source Admin Tools!](#)

Features

[Love Open Source? Try These 10 Cool Apps!](#)

The following open source applications will make your life way easier... ..

[10 Of The Best Open Source Admin Tools!](#)

Open source has a whole galaxy of tools to ease the burden on admins, we have compiled only the best ones here!...

[10 Most Awesome Cloud IDEs For Web Developers!](#)

Looking for a cloud IDE for your preferred platform? Read on... ..

[10 Amazing Open Source Tools To Make Life Easier For Web Designers!](#)

Open source tools are loved by one and all, not just because they are free, but also because they offer tremendous functionality! ...

[The Best 20 Open Source Security Apps To Protect Your System And More!](#)

It must be noted that not all of these apps are OS Independent. While some work on Linux, others are for Windows and so on. ...

[11 Online Tools For Performing Cross Browser Tests!](#)

Why look for other options when you can just test your apps and websites with different browsers online?... ..

[These 10 Online Compilers Allow You To Write Your Code Directly In The Web Browser!](#)

You don't always have to download a million things in order to start coding....

[Here Are 5 Of The Best Android Hacking Tools For You To Use!](#)

Android is everywhere these days, it is only natural to be concerned of the security of your very own Android device! ...

[Here's A Collection Of 10 Essential Programming Languages And Corresponding Books To Get You Started!](#)

The path of hacking is laden with fear and anxiety. These books will keep you up to date with everything there is for you to know about hacking!...

[10 Popular FTP Clients That You Can Use!](#)

FTP has been the preferred protocol on the internet for a long time and continues to be so....

[10 Handy jQuery Snippets For Designers](#)

Do almost anything with this amazing library of snippets that we have compiled just for you!...

[Google Play Store Can Be Much Cooler With These 10 Tips And Tricks!](#)

Try these awesome tips to bring the best out of Google Play Store! ...

[7 Tutorials On PWM That Electrical Engineers Can Use!](#)

Want to know how to modulate a pulse? Here's how....

[Want To Hack Into Your Android-Powered Smartphone? Here Are 10 Neat Tips!](#)

Android is fun, what makes it even better is amazing functionality and endless customisation!...

Fix a wonky terminal

- Difficulty: Easy
- Application: bash

We've all done it - accidentally used less or cat to list a file, and ended up viewing binary instead. This usually involves all sorts of control codes that can easily screw up your terminal display. There will be beeping. There will be funny characters. There will be odd colour combinations. At the end of it, your font will be replaced with hieroglyphics and you don't know what to do. Well, bash is obviously still working, but you just can't read what's actually going on! Send the terminal an initialisation command:

```
reset
```

and all will be well again.

Creating Mozilla keywords

- Difficulty: Easy
- Application: Firefox/Mozilla

A useful feature in Konqueror is the ability to type gg onion to do a Google search based on the word onion. The same kind of functionality can be achieved in Mozilla by first clicking on Bookmarks>Manage Bookmarks and then Add a New Bookmark. Add the URL as:

```
http://www.google.com/search?q=%s
```

Now select the entry in the bookmark editor and click the Properties button. Now enter the keyword as gg (or this can be anything you choose) and the process is complete. The %s in the URL will be replaced with the text after the keyword. You can apply this hack to other kinds of sites that rely on you passing information on the URL.

Alternatively, right-click on a search field and select the menu option "Add a Keyword for this Search...". The subsequent dialog will allow you to specify the keyword to use.

Running multiple X sessions

- Difficulty: Easy
- Application: X

If you share your Linux box with someone and you are sick of continually logging in and out, you may be relieved to know that this is not really needed. Assuming that your computer starts in graphical mode (runlevel 5), by simultaneously pressing the keys Control+Alt+F1 - you will get a login prompt. Insert your login and password and then execute:

```
startx -- :1
```

to get into your graphical environment. To go back to the previous user session, press Ctrl+Alt+F7, while to get yours back press Ctrl+Alt+F8.

You can repeat this trick: the keys F1 to F6 identify six console sessions, while F7 to F12 identify six X sessions. Caveat: although this is true in most cases, different distributions can implement this feature in a different way.

Faster browsing

- Difficulty: Easy
- Application: KDE

In KDE 3.2, a little-known but useful option has been added to speed up your web browsing experience. Start the KDE Control Center and choose System > KDE performance from the sidebar. You can now select to preload Konqueror instances. Effectively, this means that Konqueror is run on startup, but kept hidden until you try to use it. When you do, it pops up almost instantaneously. Bonus!

Backup your website easily

- Difficulty: Easy
- Application: Backups

If you want to back up a directory on a computer and only copy changed files to the backup computer instead of everything with each backup, you can use the rsync tool to do this. You will need an account on the remote computer that you are backing up from. Here is the command:

```
rsync -vare ssh jono@192.168.0.2:/home/jono/importantfiles/* /home/jono/backup/
```

Here we are backing up all of the files in /home/jono/importantfiles/ on 192.168.0.2 to /home/jono/backup on the current machine.

Keeping your clock in time

- Difficulty: Easy
- Application: NTP

If you find that the clock on your computer seems to wander off the time, you can make use of a special NTP tool to ensure that you are always synchronised with the kind of accuracy that only people that wear white coats get excited about. You will need to install the ntpdate tool that is often included in the NTP package, and then you can synchronise with an NTP server:

```
ntpdate ntp.blueyonder.co.uk
```

A list of suitable NTP servers is available at www.eecis.udel.edu/~mills/ntp/clock1b.html. If you modify your boot process and scripts to include this command you can ensure that you are perfectly in time whenever you boot your computer. You could also run a cron job to update the time.

Finding the biggest files

- Difficulty: Easy
- Application: Shell

A common problem with computers is when you have a number of large files (such as audio/video clips) that you may want to get rid of. You can find the biggest files in the current directory with: (only in current directory)

```
ls -lSrH (the r causes the large files to be listed at the end, the h gives human readable output (MB and such))
```

You could also search for the biggest MP3/MPEGs:

```
ls -lSrH *.mp*
```

You can also look for the largest directories with:

```
du -kx | egrep -v "\./+/" | sort -n
```

You can find the biggest files in your home directory, (in the whole directory structure).

Manage Your Projects With These 11 Useful Tools!

Project management includes tasks like enterprise management, task management, recording etc....

[VIEW ALL](#)

Dialogue

HTC Is Strong And There Are No Plans Of Sale Now Or In Future, Says HTC's Senior Director-Marketing

Atithya Amaresh from EfyTimes had an exclusive chat with Sirpa H. Ikola, senior director, Marketing, South Asia, HTC about its devices and its plans w...



"Cloud And Hybrid Hosting Are The Way To Go!"

Diksha P Gupta from Open Source For You spoke to Anil Chandaliya, chief network administrator, ESDS, about how customers can play safe while dealing w...



News Powered by PRNewsWire

MUMBAI, 3 hours ago 43 minutes ago

Germin8 Raises \$3 Million Venture Funding From Kalaari Capital



BEIJING, Friday, March 28, 2:40 AM

Air China to Start Beijing - Vladivostok Service



BEIJING, Thursday, March 27, 8:01 PM

Discover a World of Global Talent in the Palm of Your Hand with Nokia MixRadio, Now Available in China



S-HERTOGENBOSCH, The Netherlands, Thursday, March 27, 3:49 PM

Quintiq to Embark on "Smart Planning. Smart Business." World Tour



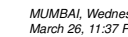
MUMBAI, Thursday, March 27, 7:02 AM

Web Services Provider, ResellerClub Launches Dedicated Servers Targeted at Enterprise Level Clients



AMSTERDAM, Thursday, March 27, 5:30 AM

Renault-Nissan Alliance Celebrates 15th Anniversary as Four Key Business Units Prepare to Converge



MUMBAI, Wednesday, March 26, 11:37 PM

GIBSS Geothermal Innovation That Cuts AC Costs in Buildings Upto 60% Bags Prestigious Bry Air Awards for Excellence in HVAC&R System Design

More News

Featured Resources:

Preventive Maintenance for Industrial & Hydraulic Hose Systems

Take proper safety precautions and identify system weaknesses before failure occurs. >>

No Nonsense XML Web Development With PHP - Free 146 Page Preview!

Learn how to put XML to practical use on your Website. >>

Videos

First Look: LG Optimus G

The phone sports a high-end display and comes powered by a powerful processor.

...



```
find ~ -type f -exec ls -s {} \; | sort -n
```

List only the top 10 biggest file.

```
find . -type f -exec ls -s {} \; | sort -nr | head -10
```

Nautilus shortcuts

- Difficulty: Easy
- Application: Nautilus

Although most file managers these days are designed to be used with the mouse, it's also useful to be able to use the keyboard sometimes. Nautilus has a few keyboard shortcuts that can have you flying through files:

- Open a location - Ctrl+L
- Open Parent folder - Ctrl+Up
- Arrow keys navigate around current folder.

You can also customise the file icons with 'emblems'. These are little graphical overlays that can be applied to individual files or groups. Open the Edit > Backgrounds and Emblems menu item, and drag-and-drop the images you want.

Defrag your databases

- Difficulty: Easy
- Application: MySQL

Whenever you change the structure of a MySQL database, or remove a lot of data from it, the files can become fragmented resulting in a loss of performance, particularly when running queries. Just remember any time you change the database to run the optimiser:

```
mysqlcheck -o
```

You may also find it worth your while to defragment your database tables regularly if you are using VARCHAR fields: these variable-length columns are particularly prone to fragmentation.

Quicker emails

- Difficulty: Easy
- Application: KMail

Can't afford to waste three seconds locating your email client? Can't be bothered finding the mouse under all those gently rotting mountains of clutter on your desk? Whatever you are doing in KDE, you are only a few keypresses away from sending a mail. Press Alt+F2 to bring up the 'Run command' dialog.

Press return and KMail will automatically fire up, ready for your words of wisdom. You don't even need to fill in the entire email address. This also works for Internet addresses: try typing www.slashdot.org to launch Konqueror.

Parallelise your build

- Difficulty: Easy
- Application: GCC

If you're running a multiprocessor system (SMP) with a moderate amount of RAM, you can usually see significant benefits by performing a parallel make when building code. Compared to doing serial builds when running make (as is the default), a parallel build is a vast improvement. To tell make to allow more than one child at a time while building, use the -j switch:

```
make -j4; make -j4 modules
```

Save battery power

- Difficulty: Intermediate
- Application: hdparm

You are probably familiar with using hdparm for tuning a hard drive, but it can also save battery life on your laptop, or make life quieter for you by spinning down drives.

```
hdparm -y /dev/hdb
hdparm -Y /dev/hdb
hdparm -S 36 /dev/hdb
```

In order, these commands will: cause the drive to switch to Standby mode, switch to Sleep mode, and finally set the Automatic spindown timeout. This last includes a numeric variable, whose units are blocks of 5 seconds (for example, a value of 12 would equal one minute).

Incidentally, this habit of specifying spindown time in blocks of 5 seconds should really be a contender for a special user-friendliness award - there's probably some historical reason for it, but we're stumped. Write in and tell us if you happen to know where it came from!

Wireless speed management

- Difficulty: Intermediate
- Application: iwconfig

The speed at which a piece of radio transmission/receiver equipment can communicate with another depends on how much signal is available. In order to maintain communications as the available signal fades, the radios need to transmit data at a slower rate. Normally, the radios attempt to work out the available signal on their own and automatically select the fastest possible speed. In fringe areas with a barely adequate signal, packets may be needlessly lost while the radios continually renegotiate the link speed. If you can't add more antenna gain, or reposition your equipment to achieve a better enough signal, consider forcing your card to sync at a lower rate. This will mean fewer retries, and can be substantially faster than using a continually flip-flopping link. Each driver has its own method for setting the link speed. In Linux, set the link speed with iwconfig:

```
iwconfig eth0 rate 2M
```

This forces the radio to always sync at 2Mbps, even if other speeds are available. You can also set a particular speed as a ceiling, and allow the card to automatically scale to any slower speed, but go no faster. For example, you might use this on the example link above:

```
iwconfig eth0 rate 5.5M auto
```

Using the auto directive this way tells the driver to allow speeds up to 5.5Mbps, and to run slower if necessary, but will never try to sync at anything faster. To restore the card to full auto scaling, just specify auto by itself:

```
iwconfig eth0 rate auto
```

Cards can generally reach much further at 1Mbps than they can at 11Mbps. There is a difference of 12dB between the 1Mbps and 11Mbps ratings of the Orinoco card - that's four times the potential distance just by dropping the data rate!

» **Create QR-Codes For Free**
TEC-IT releases the freeware QR-Code Studio to provide a quick and convenient way of QR code creation for every application scenario....



MWC 2014

» **MWC 2014: Tablet Lets People Feel Textures On Its Screen**
Now feel what you see on your tablet, by way of ultrasonic waves....



» **MWC 2014: 4K Android Tablet Games To Kill Consoles, iPad**
Tablet makers like Samsung want to beat the iPad by making 4K tabs. ...




EFY India


Like

11,629 people like EFY India.



Facebook social plugin

A SIMPLE WAY TO STAY UPDATED WITH ELECTRONICS INDUSTRY



India's First Electronics Sourcing Magazine

SUBSCRIBE IT

Want to invest in the Electronics Industry?

Comments

- » **David John said:** "Good news.This is a great post. ..." on [Car Rental Service Implements ...](#) '
- » **Deni said:** "excellent" on [50 Best Hacking Tools!](#) '

Events

» [19th Consumer Electronic Imaging Fair To Be Held On ...](#)

[VIEW ALL](#)

Unclog open ports

- Difficulty: Intermediate
- Application: netstat

Generating a list of network ports that are in the Listen state on a Linux server is simple with netstat:

```
root@catlin:~# netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:5280 0.0.0.0:* LISTEN 698/perl
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 217/httpd
tcp 0 0 10.42.3.2:53 0.0.0.0:* LISTEN 220/named
tcp 0 0 10.42.4.6:53 0.0.0.0:* LISTEN 220/named
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN 220/named
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 200/sshd
udp 0 0 0.0.0.0:32768 0.0.0.0:* 220/named
udp 0 0 10.42.3.2:53 0.0.0.0:* 220/named
udp 0 0 10.42.4.6:53 0.0.0.0:* 220/named
udp 0 0 127.0.0.1:53 0.0.0.0:* 220/named
udp 0 0 0.0.0.0:67 0.0.0.0:* 222/dhcpd
raw 0 0 0.0.0.0:1 0.0.0.0:* 7 222/dhcpd
```

That shows you that PID 698 is a Perl process that is bound to port 5280. If you're not root, the system won't disclose which programs are running on which ports.

Faster Hard drives

- Difficulty: Expert
- Application: hdparm

You may know that the `hdparm` tool can be used to speed test your disk and change a few settings. It can also be used to optimise drive performance, and turn on some features that may not be enabled by default. Before we start though, be warned that changing drive options can cause data corruption, so back up all your important data first. Testing speed is done with:

```
hdparm -Tt /dev/hda
```

You'll see something like:

```
/dev/hda:
Timing buffer-cache reads: 128 MB in 1.64 seconds =78.05 MB/sec
Timing buffered disk reads: 64 MB in 18.56 seconds = 3.45MB/sec
```

Now we can try speeding it up. To find out which options your drive is currently set to use, just pass `hdparm` the device name:

```
hdparm /dev/hda
/dev/hda:
multcount      = 16 (on)
I/O support    = 0 (default 16-bit)
unmaskirq      = 0 (off)
using_dma      = 0 (off)
keepsettings   = 0 (off)
readonly       = 0 (off)
readahead      = 8 (on)
geometry       = 40395/16/63, sectors = 40718160, start = 0
```

This is a fairly default setting. Most distros will opt for safe options that will work with most hardware. To get more speed, you may want to enable dma mode, and certainly adjust I/O support. Most modern computers support mode 3, which is a 32-bit transfer mode that can nearly double throughput. You might want to try

```
hdparm -c3 -d1/dev/hda
```

Then rerun the speed check to see the difference. Check out the modes your hardware will support, and the `hdparm` man pages for how to set them.

Uptime on your hands

- Difficulty: Expert
- Application: Perl

In computing, wasted resources are resources that could be better spent helping you. Why not run a process that updates the titlebar of your terminal with the current load average in real-time, regardless of what else you're running?

Save this as a script called `tl`, and save it to your `~/bin` directory:

```
#!/usr/bin/perl -w

use strict;
$|++;

my $host=`bin/hostname`;
chomp $host;

while(1) {

open(LOAD,"/proc/loadavg") || die "Couldn't open /proc/loadavg: $!\n";

my @load=split(/ ./);
close(LOAD);
print "\033[0;";
print "$host: $load[0] $load[1] $load[2] at ", scalar(localtime);
print "\007";

sleep 2;
}
```

When you'd like to have your titlebar replaced with the name, load average, and current time of the machine you're logged into, just run `tl&`. It will happily go on running in the background, even if you're running an interactive program like `Vim`.

Grabbing a screenshot without X

- Difficulty: Easy
- Application: Shell

There are plenty of screen-capture tools, but a lot of them are based on X. This leads to a problem when running an X application would interfere with the application you wanted to grab - perhaps a game or even a Linux installer. If you use the venerable `ImageMagick` import command though, you can grab from an X session via the console. Simply go to a virtual terminal (`Ctrl+Alt+F1` for example) and enter the following:

```
chvt 7; sleep 2; import -display :0.0 -window root sshot1.png; chvt 1;
```

The `chvt` command changes the virtual terminal, and the `sleep` command gives it a while to redraw the screen. The `import` command then captures the whole display and saves it to a file before the final `chvt` command sticks you back in the virtual terminal again. Make sure you type the whole command on one line.

This can even work on Linux installers, many of which leave a console running in the background - just load up a floppy/CD with `import` and the few libraries it requires for a first-rate run-anywhere screen grabber.

Access your programs remotely

- Difficulty: Easy
- Application: X

If you would like to lie in bed with your Linux laptop and access your applications from your Windows machine, you can do this with SSH. You first need to enable the following setting in `/etc/ssh/sshd_config`:

```
X11Forwarding yes
```

We can now run The GIMP on 192.168.0.2 with:

```
ssh -X 192.168.0.2 gimp
```

Making man pages useful

- Difficulty: Easy
- Application: man

If you are looking for some help on a particular subject or command, man pages are a good place to start. You normally access a man page with `man`, but you can also search the man page descriptions for a particular keyword. As an example, search for man pages that discuss logins:

```
man -k login
```

When you access a man page, you can also use the forward slash key to search for a particular word within the man page itself. Simply press `/` on your keyboard and then type in the search term.

Talk to your doctor!

- Difficulty: Easy
- Application: Emacs

To say that Emacs is just a text editor is like saying that a Triumph is just a motorcycle, or the World Cup is just some four-yearly football event. True, but simplified juuust a little bit. An example? Open the editor, press the Esc key followed by X and then enter in doctor: you will be engaged in a surreal conversation by an imaginary and underskilled psychotherapist. And if you want to waste your time in a better way

```
Esc-X tetris
```

will transform your 'editor' into the old favourite arcade game.

Does the madness stop there? No! Check out your distro's package list to see what else they've bundled for Emacs: here at LXF Towers we've got chess, Perl integration, IRC chat, French translation, HTML conversion, a Java development environment, smart compilation, and even something called a "semantic bovinator". We really haven't the first clue what that last one does, but we dare you to try it out anyway! (Please read the disclaimer first!)

Super cow powers

- Difficulty: Easy
- Application: Debian

A strange but endearing hidden feature within the highly regarded apt-get tool in Debian is its secret cow powers. Type the following command to experience the wrath of the super cow powers:

```
apt-get moo
```

Some people really have too much time on their hands...

Generating package relationship diagrams

- Difficulty: Easy
- Application: Debian

The most critical part of the Debian system is the ability to install a package and have the dependencies satisfied automatically. If you would like a graphical representation of the relationships between these packages (this can be useful for seeing how the system fits together), you can use the Graphviz package from Debian non-free (apt-get install graphviz) and the following command:

```
apt-cache dotty > debian.dot
```

The command generated the graph file which can then be loaded into dotty:

```
dotty debian.dot
```

Unmount busy drives

- Difficulty: Easy
- Application: bash

You are probably all too familiar with the situation - you are trying to unmount a drive, but keep getting told by your system that it's busy. But what application is tying it up? A quick one-liner will tell you:

```
lsof +D /mnt/windows
```

This will return the command and process ID of any tasks currently accessing the `/mnt/windows` directory. You can then locate them, or use the `kill` command to finish them off.

Text file conversion

- Difficulty: Easy
- Application: recode

`recode` is a small utility that will save you loads of effort when using text files created on different platforms. The primary source of discontent is line breaks. In some systems, these are denoted with a line-feed character. In others, a carriage return is used. In still more systems, both are used. The end result is that if you are swapping text from one platform to another, you end up with too many or too few line breaks, and lots of strange characters besides.

However, the command parameters of `recode` are a little arcane, so why not combine this hack with HACK 26 in this feature, and set up some useful aliases:

```
alias dos2unix='recode dos/CR-LF..11'
alias unix2win='recode 11..windows-1250'
alias unix2dos='recode 11..dos/CR-LF'
```

There are plenty more options for `recode` - it can actually convert between a whole range of character sets. Check out the man pages for more information.

Listing today's files only

- Difficulty: Easy
- Application: Various

You are probably familiar with the problem. Sometime earlier in the day, you created a text file, which now is urgently required. However, you can't remember what ridiculous name you gave it, and being a typical geek, your home folder is full of 836 different files. How can you find it? Well, there are various ways, but this little tip shows you the power of pipes and joining together two powerful shell commands:

```
ls -al --time-style=+%D | grep `date +%D`
```

The parameters to the `ls` command here cause the timestamp to be output in a particular format. The cunning bit is that the output is then passed to `grep`. The `grep` parameter is itself a command (executed because of the backticks), which substitutes the current date into the string to be matched. You could easily modify it to search specifically for other dates, times, filesize or whatever. Combine it with HACK 26 to save typing!

Avoid common mistypes and long commands

- Difficulty: Easy
- Application: Shell

The `alias` command is useful for setting up shortcuts for long commands, or even more clever things. From HACK 25, we could make a new command, `lsnew`, by doing this:

```
alias lsnew=" ls -al --time-style=+%D | grep `date +%D` "
```

But there are other uses of `alias`. For example, common mistyping mistakes. How many times have you accidentally left out the space when changing to the parent directory? Worry no more!

```
alias cd..="cd .."
```

Alternatively, how about rewriting some existing commands?

```
alias ls="ls -al"
```

saves a few keypresses if, like us, you always want the complete list.

To have these shortcuts enabled for every session, just add the `alias` commands to your user `.bashrc` file in your home directory.

Alter Mozilla's secret settings

- Difficulty: Easy
- Application: Mozilla

If you find that you would like to change how Mozilla works but the preferences offer nothing by way of clickable options that can help you, there is a special mode that you can enable in Mozilla so that you can change anything. To access it, type this into the address bar:

```
about:config
```

You can then change each setting that you are interested in by changing the Value field in the table.

Other interesting modes include general information (`about:`), details about plugins (`about:plugins`), credits information (`about:credits`) and some general wisdom (`about:mozilla`).

A backdrop of stars

- Difficulty: Easy
- Application: KStars

You may already have played with KStars, as it was included with the astronomy software that featured in LXF50's Roundup; but how about creating a KStars backdrop image that's updated every time you start up?

KStars can be run with the `--dump` switch, which dumps out an image from your startup settings, but doesn't load the GUI at all. You can create a script to run this and generate a desktop image, which will change every day (or you can just use this method to generate images).

Run KStars like this:

```
kstars --dump --width 1024 --height 768 --filename = ~/kstarsback.png
```

You can add this to a script in your `~/kde/Autostart` folder to be run at startup. Find the file in Konqueror, drag it to the desktop and select 'Set as wallpaper' to use it as a randomly generated backdrop.

Open an SVG directly

- Difficulty: Easy
- Application: Inkscape

You can run Inkscape from a shell and immediately edit a graphic directly from a URL. Just type:

```
inkscape http://www.somehost.com/graphic.svg
```

Remember to save it as something else though!

Editing without an editor

- Difficulty: Intermediate
- Application: Various

Very long files are often hard to manipulate with a text editor. If you need to do it regularly, chances are you'll find it much faster to use some handy command-line tools instead, like in the following examples.

To print columns eg 1 and 3 from a file `file1` into `file2`, we can use `awk`:

```
awk '{print $1, $3}' file1 > file2
```

To output only characters from column 8 to column 15 of file1, we can use cut:

```
cut -c 8-15 file1 > file2
```

To replace the word word1 with the word word2 in the file file1, we can use the sed command:

```
sed "s/word1/word2/g" file1 > file2
```

This is often a quicker way to get results than even opening a text editor.

Backup selected files only

- Difficulty: Intermediate
- Application: tar

Want to use tar to backup only certain files in a directory? Then you'll want to use the -T flag as follows. First, create a file with the file you want to backup:

```
cat >> /etc/backup.conf
# /etc/passwd
# /etc/shadow
# /etc/yp.conf
# /etc/sysctl.conf
EOF
```

Then run tar with the -T flag pointing to the file just created:

```
tar -cjf bck-etc-`date +%Y-%m-%d`.tar.bz2 -T /etc/backup.conf
```

Now you have your backup.

Merging columns in files

- Difficulty: Intermediate
- Application: bash

While splitting columns in files is easy enough, merging them can be complicated. Below is a simple shell script that does the job:

```
#!/bin/sh
length=wc -l $1 | awk '{print $1}'
count=1
[ -f $3 ] && echo "Optionally removing $3" && rm -i $3
while [ "$count" -le "$length" ] ; do
  a=`head - $count $1 | tail -1`
  b=`head - $count $2 | tail -1`
  echo "$a      $b" >> $3
  count=`expr $count + 1`
done
```

Give to this script the name merge.sh and make it executable with:

```
chmod u+x merge.sh
```

Now, if you want to merge the columns of file1 and file2 into file3, it's just matter of executing

```
/path/to/merge.sh file1 file2 file3
```

where /path/to has to be replaced with the location of merge.sh in your filesystem.

Case sensitivity

- Difficulty: Intermediate
- Application: bash

Despite the case of a word not making any difference to other operating systems, in Linux "Command" and "command" are different things. This can cause trouble when moving files from Windows to Linux. tr is a little shell utility that can be used to change the case of a bunch of files.

```
#!/bin/sh
for i in `ls -l`; do
  file1=`echo $i | tr [A-Z] [a-z]`
  mv $i $file1 2>/dev/null
done
```

By executing it, FILE1 and file2 will be renamed respectively file1 and file2.

Macros in Emacs

- Difficulty: Intermediate
- Application: Emacs

When editing files, you will often find that the tasks are tedious and repetitive, as LXF's Production Editor knows only too well! To spare your time, you can record a macro. In Emacs, you will have to go through the following steps:

1. Press Ctrl+X to start recording.
2. Insert all the keystrokes and commands that you want
3. Press Ctrl+X to stop when you're done.

Now, you can execute that with

```
Ctrl -u Ctrl -x e
```

where is the number of times you want to execute the macro. If you enter a value of 0, the macro will be executed until the end of the file is reached. Ctrl -x e is equivalent to Ctrl -u 1 Ctrl-x e.

Replacing same text in multiple files

- Difficulty: Intermediate
- Application: find/Perl

If you have text you want to replace in multiple locations, there are several ways to do this. To replace the text Windows with Linux in all files in current directory called test[something] you can run this:

```
perl -i -pe 's/Windows/Linux/;' test*
```

To replace the text Windows with Linux in all text files in current directory and down you can run this:


```
find . -name '*.txt' -print | xargs perl -pi -e 's/Windows/Linux/ig' *.txt
```

Or if you prefer this will also work, but only on regular files:

```
find -type f -name '*.txt' -print0 | xargs --null perl -pi -e 's/Windows/Linux/'
```

Saves a lot of time and has a high guru rating!

Simple spam killing

- Difficulty: Intermediate
- Application: KMail

Spam, or unsolicited bulk email, is such a widespread problem that almost everyone has some sort of spam protection now, out of necessity. Most ISPs include spam filtering, but it isn't set to be too aggressive, and most often simply labels the spam, but lets it through (ISPs don't want to be blamed for losing your mails). The result is that, while you may have anti-spam stuff set up on the client-side, you can make its job easier by writing a few filters to remove the spam that's already labelled as such. The label is included as a header. In KMail, you can just create a quick filter to bin your mail, or direct it to a junk folder. The exact header used will depend on the software your ISP is using, but it's usually something like X-Spam-Flag = YES for systems like SpamAssassin. Simply create a filter in KMail, choose Match Any of the Following and type in the header details and the action you require. Apply the filter to incoming mail, and you need never be troubled by about half the volume of your spam ever again.

Read OOo docs without OOo

- Difficulty: Intermediate
- Application: OpenOffice.org

Have you ever been left with an OOo document, but no OpenOffice.org in which to read it? Thought you saved it out as plain text (.txt), but used the StarOffice .sxw format instead? The text can be rescued. Firstly, the sxw file is a zip archive, so unzip it:

```
unzip myfile.sxw
```

The file you want is called 'content.xml'. Unfortunately, it's so full of xml tags it's fairly illegible, so filter them out with some Perl magic:

```
cat content.xml | perl -p -e "s/<[^>]*>/ /g;s/\n/ /g;s/ +/ /g;"
```

It may have lost lots of formatting, but at least it is now readable.

Find and execute

- Difficulty: Intermediate
- Application: find

The find command is not only useful for finding files, but is also useful for processing the ones it finds too. Here is a quick example.

Suppose we have a lot of tarballs, and we want to find them all:

```
find . -name '*.gz'
```

will locate all the gzip archives in the current path. But suppose we want to check they are valid archives? The gunzip -vt option will do this for us, but we can cunningly combine both operations, using xargs:

```
find . -name '*.gz' | xargs gunzip -vt
```

In case the files contain spaces, these commands won't work. The following variant takes care about this case:

```
find . -name '*.gz' -print0 | xargs -0 gunzip -vt
```

Use the correct whois server

- Difficulty: Intermediate
- Application: whois

The whois command is very useful for tracking down Internet miscreants and the ISPs that are supplying them with service. Unfortunately, there are many whois servers, and if you are querying against a domain name, you often have to use one which is specific to the TLD they are using. However, there are some whois proxies that will automatically forward your query on to the correct server. One of these is available at <http://whois.geektools.com>

```
whois -h whois.geektools.com plop.info
```

Where did that drive mount?

- Difficulty: Intermediate
- Application: bash

A common problem with people who have lots of mountable devices (USB drives, flash memory cards, USB key drives) is working out where that drive you just plugged in has ended up?

Practically all devices that invoke a driver - such as usb-storage - will dump some useful information in the logs. Try

```
dmesg | grep SCSI
```

This will filter out recognised drive specs from the dmesg output. You'll probably turn up some text like:

```
SCSI device sda: 125952 512-byte hdwr sectors (64 MB)
```

So your device is at sda.

Autorun USB devices

- Difficulty: Expert
- Application: hotplug scripts

Want to run a specific application whenever a particular device is added? The USB hotplug daemon can help you! This service is notified when USB devices are added to the system. For devices that require kernel drivers, the hotplug daemon will call a script by the same name in /etc/hotplug/usb/, for example, a script called usb-storage exists there. You can simply add your own commands to the end of this script (or better still, tag a line at the end of it to execute a script elsewhere). Then you can play a sound, autosync files, search for pictures or whatever.

For devices that don't rely on kernel drivers, a lookup table is used matching the USB product and manufacturer ID. Many distros already set this up to do something, but you can customise these scripts pretty easily. See <http://photo.sourceforge.net/?selected=sync> for an example of what can be done.

Rename and resize images

- Difficulty: Expert
- Application: bash

Fond of your new camera but can't put up with the terrible names? Do you want also to prepare them for publishing on the web? No problem, a simple bash script is what you need:

```
#!/bin/sh
counter=1
root=mypict
resolution=400x300
for i in `ls -l $1/*.jpg`; do
    echo "Now working on $i"
    convert -resize $resolution $i ${root}_${counter}.jpg
    counter=`expr $counter + 1`
done
```

Save the script in a file called `picturename.sh` and make it executable with

```
chmod u+x picturename.sh
```

and store it somewhere in your path. Now, if you have a bunch of `.jpg` files in the directory `/path/to/picdir`, all you have to do is to execute

```
picturename.sh /path/to/picdir
```

and in the current directory you'll find `mypict_1.jpg`, `mypict_2.jpg` etc, which are the resized versions of your original ones. You can change the script according to your needs.

Secure logout

- Difficulty: Easy
- Application: bash

When you are using a console on a shared machine, or indeed, just on your own desktop, you may find that when you logout, the screen still shows a trace of who was logged in and what you were doing. A lot of distros will clear the screen, but some don't. You can solve this by editing your `~/bash_logout` file and adding the command:

```
clear
```

You can add any other useful commands here too.

Transferring files without ftp or scp

- Difficulty: Easy
- Application: netcat

Need to transfer a directory to another server but do not have FTP or SCP access? Well this little trick will help out using the netcat utility. On the destination server run:

```
nc -l -p 1234 | uncompress -c | tar xvpf -
```

And on the sending server run:

```
tar cfp - /some/dir | compress -c | nc -w 3 [destination] 1234
```

Now you can transfer directories without FTP and without needing root access.

Backing up a Debian package list

- Difficulty: Easy
- Application: Debian

If you are running Debian and have lost track of which packages you are running, it could be useful to get a backup of your currently installed packages. You can get a list by running:

```
dpkg --get-selections > debianlist.txt
```

This will put the entire list in `debianlist.txt`. You could then install the same packages on a different computer with:

```
dpkg --set-selections < debianlist.txt
```

You should bear in mind that you would also need to copy over configuration files from `/etc` when copying your system to a new computer.

To actually install the selections, use:

```
apt-get -u dselect-upgrade.
```

Hardening ssh

- Difficulty: Easy
- Application: ssh

Although SSH is a pretty secure way to connect to your server, there are two simple changes you can make that will boost its security even further. First, you almost certainly don't want people logging in directly as root - instead, they should logon as a normal user, then use the `su` command to switch over. You can change this simply in the `/etc/ssh/ssh_config` file by adding the line:

```
PermitRootLogin no
```

Now the only way to get root privileges is through `su`, which means crackers now need to break two passwords to get full access. While you are editing that file, find the line which says:

```
Protocol 2, 1
```

And change it to:

```
Protocol 2
```

This removes the option to fallback on the original SSH protocol, now considered very vulnerable.

Stop replying to pings

- Difficulty: Easy
- Application: sysctl

While ping is a very useful command for discovering network topology, the disadvantage is that it does just that, and makes it easier for hackers on the network to target live servers. But you can tell Linux to ignore all pings - the server simply won't respond. There are a number of ways to achieve this, but the best is to use `sysctl`. To turn off ping replies:

```
sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

To turn it back on, again use:

```
sysctl -w net.ipv4.icmp_echo_ignore_all=0
```

If turning off ping is too severe for you, take a look at the next hack.

Slow down ping rates

- Difficulty: Easy
- Application: sysctl

You may want to keep the ability to reply to pings, but protect yourself from a form of attack known as a 'ping flood'. So how can you manage such a feat? The easiest way is to slow down the rate at which the server replies to pings. They are still valid, but won't overload the server:

```
sysctl -w net.ipv4.icmp_echo_reply_rate=10
```

This slows the rate at which replies are sent to a single address.

Clean up KDE on logout

- Difficulty: Easy
- Application: bash

On Windows there are plenty of programs that do stuff like clean out your web cache, remove temporary files and all sorts of other stuff when you logout. Wouldn't it be cool to do this on Linux too? With KDE, you don't need to even install any new software, as the startkde script will automatically run scripts you put in special places.

First, you need to create a directory called shutdown in your .kde directory:

```
mkdir /home/username/.kde/shutdown
```

Now create a script to do any stuff you like on shutdown. Here is an example:

```
#!/bin/bash
#clear up temp folder
rm -rf ~/tmp/*
#clear out caches
rm -rf ~/.ee/minis/*
rm -rf ~/.kde/share/cache/http/*
# delete konqueror form completions
rm ~/.kde/share/apps/khtml/formcompletions
```

Now make sure you set the correct permissions:

```
chmod ug+x ~/.kde/shutdown/cleanup.sh
```

(or whatever you called it). As well as cleaning up sensitive files, you can also have global shutdown scripts for all users, by placing the script in your default KDE folder, in a subfolder called shutdown. To find out which is your default KDE directory, try:

```
kde-config --path exe
```

Password-less ssh

- Difficulty: Intermediate
- Application: ssh

Tired of typing your password every time you log into the server? ssh also supports keys, so you'll only have to type in your password when you log in to the desktop. Generate a keypair on your desktop machine:

```
ssh-keygen -t dsa -C your.email@address
```

Enter a passphrase for your key. This puts the secret key in ~/.ssh/id_dsa and the public key in ~/.ssh/id_dsa.pub. Now see whether you have an ssh-agent running at present:

```
echo $SSH_AGENT_PID
```

Most window managers will run it automatically if it's installed. If not, start one up:

```
eval $(ssh-agent)
```

Now, tell the agent about your key:

```
ssh-add
```

and enter your passphrase. You'll need to do this each time you log in; if you're using X, try adding

```
SSH_ASKPASS=ssh-askpass ssh-add
```

to your .xsession file. (You may need to install ssh-askpass.) Now for each server you log into, create the directory ~/.ssh and copy the file ~/.ssh/id_dsa.pub into it as ~/.ssh/authorized_keys . If you started the ssh-agent by hand, kill it with

```
ssh-agent -k
```

when you log out.

Using rsync over ssh

- Difficulty: Intermediate
- Application: Shell

Keep large directory structures in sync quickly with rsync. While tar over SSH is ideal for making remote copies of parts of a filesystem, rsync is even better suited for keeping the filesystem in sync between two machines. To run an rsync over SSH, pass it the -e switch, like this:

```
rsync -ave ssh greendome:/home/ftp/pub/ /home/ftp/pub/
```

Note the trailing / on the file spec from the source side (on greendome.) On the source spec, a trailing / tells rsync to copy the contents of the directory, but not the directory itself. To include the directory as the top level of what's being copied, leave off the /:

```
rsync -ave ssh bcnu:/home/six .
```

This will keep a copy of the ~/six/ directory on village in sync with whatever is present on bcnu:/home/six/. By default, rsync will only copy files and directories, but not remove them from the destination copy when they are removed from the source. To keep the copies exact, include the --delete flag:

```
rsync -ave ssh --delete greendome:~one/reports .
```

Now when old reports are removed from `~one/reports/` on greendome, they're also removed from `~six/public_html/reports/` on the synced version, every time this command is run. If you run a command like this in cron, leave off the `y` switch. This will keep the output quiet (unless `rsync` has a problem running, in which case you'll receive an email with the error output). Using `SSH` as your transport for `rsync` traffic has the advantage of encrypting the data over the network and also takes advantage of any trust relationships you already have established using `SSH` client keys.

Asset scanning

- Difficulty: Intermediate
- Application: nmap

Normally, when people think of using `nmap`, they assume it's used to conduct some sort of nefarious network reconnaissance in preparation for an attack. But as with all powerful tools, `nmap` can be made to wear a white hat, as it's useful for far more than breaking into networks. For example, simple `TCP` connect scans can be conducted without needing root privileges:

```
nmap rigel
```

`nmap` can also scan ranges of IP addresses by specifying the range or using `CIDR` notation:

```
nmap 192.168.0.1-254
nmap 192.168.0/24
```

`nmap` can provide much more information if it is run as root. When run as root, it can use special packets to determine the operating system of the remote machine by using the `-O` flag. Additionally, you can do half-open `TCP` scanning by using the `-sS` flag. When doing a half-open scan, `nmap` will send a `SYN` packet to the remote host and wait to receive the `ACK` from it; if it receives an `ACK`, it knows that the port is open. This is different from a normal three-way `TCP` handshake, where the client will send a `SYN` packet and then send an `ACK` back to the server once it has received the initial server `ACK`. Attackers typically use this option to avoid having their scans logged on the remote machine.

```
nmap -sS -O rigel
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on rigel.nnc (192.168.0.61):
(The 1578 ports scanned but not shown below are in state: filtered)
Port      State      Service
7/tcp     open      echo
9/tcp     open      discard
13/tcp    open      daytime
19/tcp    open      chargen
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
37/tcp    open      time
79/tcp    open      finger
111/tcp   open      sunrpc
512/tcp   open      exec
513/tcp   open      login
514/tcp   open      shell
587/tcp   open      submission
7100/tcp  open      font-service
32771/tcp open      sometimes-rpc5
32772/tcp open      sometimes-rpc7
32773/tcp open      sometimes-rpc9
32774/tcp open      sometimes-rpc11
32777/tcp open      sometimes-rpc17
Remote operating system guess: Solaris 9 Beta through Release on SPARC
Uptime 44.051 days (since Sat Nov  1 16:41:50 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 166 seconds
```

With `OS` detection enabled, `nmap` has confirmed that the `OS` is `Solaris`, but now you also know that it's probably `Version 9` running on a `SPARC` processor.

One powerful feature that can be used to help keep track of your network is `nmap`'s `XML` output capabilities. This is activated by using the `-oX` command-line switch, like this:

```
nmap -sS -O -oX scandata.xml rigel
```

This is especially useful when scanning a range of IP addresses or your whole network, because you can put all the information gathered from the scan into a single `XML` file that can be parsed and inserted into a database. Here's what an `XML` entry for an open port looks like:

`nmap` is a powerful tool. By using its `XML` output capabilities, a little bit of scripting, and a database, you can create an even more powerful tool that can monitor your network for unauthorized services and machines.

Backup your bootsector

- Difficulty: Expert
- Application: Shell

Messing with bootloaders, dual-booting and various other scary processes can leave you with a messed up bootsector. Why not create a backup of it while you can:

```
dd if=/dev/hda of=bootsector.img bs=512 count=1
```

Obviously you should change the device to reflect your boot drive (it may be `sda` for `SCSI`). Also, be very careful not to get things the wrong way around - you can easily damage your drive! To restore use:

```
dd if=bootsector.img of=/dev/hda
```

Protect log files

- Difficulty: Expert
- Application: Various

During an intrusion, an attacker will more than likely leave telltale signs of his actions in various system logs: a valuable audit trail that should be protected. Without reliable logs, it can be very difficult to figure out how the attacker got in, or where the attack came from. This info is crucial in analysing the incident and then responding to it by contacting the appropriate parties involved. But, if the break-in is successful, what's to stop him from removing the traces of his misbehaviour?

This is where file attributes come in to save the day (or at least make it a little better). Both `Linux` and the `BSDs` have the ability to assign extra attributes to files and directories. This is different from the standard `Unix` permissions scheme in that the attributes set on a file apply universally to all users of the system, and they affect file accesses at a much deeper level than file permissions or `ACLs`. In `Linux`, you can see and modify the attributes that are set for a given file by using the `lsattr` and `chattr` commands, respectively. At the time of this writing, file attributes in `Linux` are available only when using the `ext2` and `ext3` filesystems. There are also kernel patches available for attribute support in `XFS` and `ReiserFS`. One useful attribute for protecting log files is `append-only`. When this attribute is set, the file cannot be deleted, and writes are only allowed to append to the end of the file.

To set the `append-only` flag under `Linux`, run this command:

```
chattr +a filename
```

See how the +a attribute works: create a file and set its append-only attribute:

```
touch /var/log/logfile
echo "append-only not set" > /var/log/logfile
chattr +a /var/log/logfile
echo "append-only set" > /var/log/logfile
bash: /var/log/logfile: Operation not permitted
```

The second write attempt failed, since it would overwrite the file. However, appending to the end of the file is still permitted:

```
echo "appending to file" >> /var/log/logfile
cat /var/log/logfile
append-only not set
appending to file
```

Obviously, an intruder who has gained root privileges could realise that file attributes are being used and just remove the append-only flag from our logs by running `chattr -a`. To prevent this, we need to disable the ability to remove the append-only attribute. To accomplish this under Linux, use its capabilities mechanism.

The Linux capabilities model divides up the privileges given to the all-powerful root account and allows you to selectively disable them. In order to prevent a user from removing the append-only attribute from a file, we need to remove the `CAP_LINUX_IMMUTABLE` capability. When present in the running system, this capability allows the append-only attribute to be modified. To modify the set of capabilities available to the system, we will use a simple utility called `lcap` (<http://packetstormsecurity.org/linux/admin/lcap-0.0.3.tar.bz2>).

To unpack and compile the tool, run this command:

```
tar xvfj lcap-0.0.3.tar.bz2 && cd lcap-0.0.3 && make
```

Then, to disallow modification of the append-only flag, run:

```
./lcap CAP_LINUX_IMMUTABLE
./lcap CAP_SYS_RAWIO
```

The first command removes the ability to change the append-only flag, and the second removes the ability to do raw I/O. This is needed so that the protected files cannot be modified by accessing the block device they reside on. It also prevents access to `/dev/mem` and `/dev/kmem`, which would provide a loophole for an intruder to reinstate the `CAP_LINUX_IMMUTABLE` capability. To remove these capabilities at boot, add the previous two commands to your system startup scripts (eg `/etc/rc.local`). You should ensure that capabilities are removed late in the boot order, to prevent problems with other startup scripts. Once `lcap` has removed kernel capabilities, they can be reinstated only by rebooting the system.

Before doing this, you should be aware that adding append-only flags to your log files will most likely cause log rotation scripts to fail. However, doing this will greatly enhance the security of your audit trail, which will prove invaluable in the event of an incident.

Automatically encrypted connections

- Difficulty: Expert
- Application: FreeS/WAN

One particularly cool feature supported by FreeS/WAN is opportunistic encryption with other hosts running FreeS/WAN. This allows FreeS/WAN to transparently encrypt traffic between all hosts that also support opportunistic encryption. To do this, each host must have a public key generated to use with FreeS/WAN. This key can then be stored in a DNS TXT record for that host. When a host that is set up for opportunistic encryption wishes to initiate an encrypted connection with another host, it will look up the host's public key through DNS and use it to initiate the connection.

To begin, you'll need to generate a key for each host that you want to use this feature with. You can do that by running the following command:

```
ipsec newhostkey --output /tmp/`hostname`.key
```

Now you'll need to add the contents of the file that was created by that command to `/etc/ipsec.secrets`:

```
cat /tmp/`hostname`.key >> /etc/ipsec.secrets
```

Next, you'll need to generate a TXT record to put into your DNS zone. You can do this by running a command similar to this one:

```
ipsec showhostkey --txt @colossus.nnc
```

Now add this record to your zone and reload it. You can verify that DNS is working correctly by running this command:

```
ipsec verify
Checking your system to see if IPsec got installed and started correctly
Version check and ipsec on-path [OK]
Checking for KLIPS support in kernel [OK]
Checking for RSA private key (/etc/ipsec.secrets) [OK]
Checking that pluto is running [OK]
DNS checks.
Looking for TXT in forward map: colossus [OK]
Does the machine have at least one non-private address [OK]
```

Now just restart FreeS/WAN - you should now be able to connect to any other host that supports opportunistic encryption. But what if other hosts want to connect to you? To allow this, you'll need to create a TXT record for your machine in your reverse DNS zone.

You can generate the record by running a command similar to this:

```
ipsec showhostkey --txt 192.168.0.64
```

Add this record to the reverse zone for your subnet, and other machines will be able to initiate opportunistic encryption with your machine. With opportunistic encryption in use, all traffic between the hosts will be automatically encrypted, protecting all services simultaneously.

Eliminate suid binaries

- Difficulty: Intermediate
- Application: find

If your server has more shell users than yourself, you should regularly audit the `setuid` and `setgid` binaries on your system. Chances are you'll be surprised at just how many you'll find. Here's one command for finding all of the files with a `setuid` or `setgid` bit set:

```
find / -perm +6000 -type f -exec ls -ld {} \; > setuid.txt &
```

This will create a file called `setuid.txt` that contains the details of all of the matching files present on your system. To remove the `s` bits of any tools that you don't use, type:

```
chmod a-s program
```

Mac filtering Host AP

- Difficulty: Expert
- Application: `iwpriv`

While you can certainly perform MAC filtering at the link layer using `iptables` or `ebtables`, it is far safer to let Host AP do it for you. This not only blocks

traffic that is destined for your network, but also prevents miscreants from even associating with your station. This helps to preclude the possibility that someone could still cause trouble for your other associated wireless clients, even if they don't have further network access.

When using MAC filtering, most people make a list of wireless devices that they wish to allow, and then deny all others. This is done using the `iwpriv` command.

```
iwpriv wlan0 addmac 00:30:65:23:17:05
iwpriv wlan0 addmac 00:40:96:aa:99:fd
...
iwpriv wlan0 maccmd 1
iwpriv wlan0 maccmd 4
```

The `addmac` directive adds a MAC address to the internal table. You can add as many MAC addresses as you like to the table by issuing more `addmac` commands. You then need to tell Host AP what to do with the table you've built. The `maccmd 1` command tells Host AP to use the table as an "allowed" list, and to deny all other MAC addresses from associating. Finally, the `maccmd 4` command boots off all associated clients, forcing them to reassociate. This happens automatically for clients listed in the table, but everyone else attempting to associate will be denied.

Sometimes, you only need to ban a troublemaker or two, rather than set an explicit policy of permitted devices. If you need to ban a couple of specific MAC address but allow all others, try this:

```
iwpriv wlan0 addmac 00:30:65:fa:ca:de
iwpriv wlan0 maccmd 2
iwpriv wlan0 kickmac 00:30:65:fa:ca:de
```

As before, you can use `addmac` as many times as you like. The `maccmd 2` command sets the policy to "deny," and `kickmac` boots the specified MAC immediately, if it happens to be associated. This is probably nicer than booting everybody and making them reassociate just to ban one troublemaker. Incidentally, if you'd like to remove MAC filtering altogether, try `maccmd 0`.

If you make a mistake typing in a MAC address, you can use the `delmac` command just as you would `addmac`, and it (predictably) deletes the given MAC address from the table. Should you ever need to flush the current MAC table entirely but keep the current policy, use this command:

```
iwpriv wlan0 maccmd 3
```

Finally, you can view the running MAC table by using `/proc`:

```
cat /proc/net/hostap/wlan0/ap_control
```

The `iwpriv` program manipulates the running Host AP driver, but doesn't preserve settings across reboots. Once you are happy with the contents of your MAC filtering table, be sure to put the relevant commands in an rc script to run at boot time.

Note that even unassociated clients can still listen to network traffic, so MAC filtering actually does very little to prevent eavesdropping. To combat passive listening techniques, you will need to encrypt your data.

Check processes not run by you

- Difficulty: Expert
- Application: bash

Imagine the scene - you read our list of Linux Format Awards nominees this month, saw Crack Attack! on there, and took it upon yourself to give it a (very) thorough testing before casting your vote in its favour. Sadly, to your shock, the game drags to a halt just as you're about to beat your uppy subordinate - what could be happening to make your machine so slow? It must be some of those other users, stealing your precious CPU time with their scientific experiments, web servers or other weird, geeky things!

OK, let's list all the processes on the box not being run by you!

```
ps aux | grep -v `whoami`
```

Or, to be a little more clever, why not just list the top ten time-wasters:

```
ps aux --sort=-%cpu | grep -m 11 -v `whoami`
```

It is probably best to run this as root, as this will filter out most of the vital background processes. Now that you have the information, you could just kill their processes, but much more dastardly is to run xeyes on their desktop. Repeatedly!

Courtesy: linuxformat

Rate this news:  (3 Votes)

 [Print](#)  [Email](#)  [Post Comment](#) (1)


 [BOOKMARK](#)    (Total Views: 17448)

1.5k

Share

- 
- 

Database Management

 [synametrics.com](#)

WinSQL - A Homogeneous Solution for Heterogeneous Environment.



1 Comments

Allan Daemon 158 days ago

In the Harding SSH I think the right file to modify is `etcsshshd_config`. The file `etcsshsh_config` is to configure the client not the server.

 [Reply](#)

Linux & Open Source News

- » [Love Open Source? Try These 10 Cool Apps!](#)
- » [10 Of The Best Open Source Admin Tools!](#)
- » [10 Most Awesome Cloud IDEs For Web Developers!](#)
- » [10 Amazing Open Source Tools To Make Life Easier For Web Designers!](#)
- » [The Best 20 Open Source Security Apps To Protect Your System And More!](#)

[home](#) [archives](#) [contact us](#) [advertise with us](#)



Magazines

Electronics for You
Open Source for You
Facts for You
Electronics Bazaar

Portals

[electronicsforu.com](#)
[efytimes.com](#)
[bpotimes.com](#)
[linuxforu.com](#)

Directories

Electronics Annual Guide

Events

EFY EXPO
EFY Awards
EduTech Expo
OSIDAYS Expo

News Verticals

Electronics
Infotech
Linux & Open Source
Consumer Electronics

Educational Institute

EFY Techcenter

Science & Technology
BPO

© Copyright 2014 EFY Enterprises Pvt. Ltd.
All rights reserved. Reproduction in whole or in part in any form or medium without written permission is prohibited.
Usage of the content from the web site is subject to Terms and Conditions