===========================================================  
Practical Linux Topics - Chris Binnie - Lengthy Commands and Some Listings  
===========================================================  
  
Chapter 1

=======  
  
# rpm -ivh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm  
  
not ether host ff:ff:ff:ff:ff:ff  
  
# iftop-f “host mail.chrisbinnie.tld and not port smtp”

dst host router.chrisbinnie.tld and src port bgpd and not host ntp.chrisbinnie.tld

src host web.chrisbinnie.tld portrange 0-1024

# cat /root/.iftoprc  
  
dns-resolution: yes  
port-resolution: yes  
show-bars: yes  
promiscuous: yes  
port-display: on  
hide-source: no  
hide-destination: no  
use-bytes: no  
sort: 2s  
line-display: one-line-both  
show-totals: yes  
log-scale: yes  
  
Chapter 2

=======  
  
# shred ­vfz ­n 25 /dev/sda3  
# shred ­vfz ­n 5 /dev/sdc  
# dd if=RANDOMDATA of=/dev/sda1 bs=<sector\_size> count=<sector\_number> seek=<sector\_where\_to\_start>  
# dd if=RANDOMDATA of=/dev/sda1 bs=512 count=501 seek=2  
# dd if=RANDOMDATA of=/dev/sda bs=<physical\_sector> count=<every\_physical\_sector> seek=0  
# echo $((24696061952 / 512))  
  
Chapter 3  
=======

# systemctl start SERVICENAME.service

# systemctl try-restart SERVICENAME.service

# service --status-all

# systemctl list-units --type service --all

# update-rc.d SERVICENAME defaults

# insserv SERVICENAME

# insserv -n

# insserv -r SERVICENAME

# systemctl enable SERVICENAME.service

# systemctl disable SERVICENAME.service

# systemctl enable SERVICENAME.service

# systemctl status SERVICENAME.service

# chkconfig --list

# systemctl list-unit-files --type service

# systemctl list-units --type service

# systemctl list-units --all

# systemctl list-unit-files --type=target

# systemctl get-default

# rm /etc/systemd/system/default.target

# ln -sf /lib/systemd/system/graphical.target /etc/systemd/system/default.target

# systemctl isolate TARGETNAME.target

# systemctl isolate multi-user.target

# systemctl rescue

# systemctl emergency

# systemd-analyze

# systemd-analyze blame

# systemd-analyze critical-chain

# systemd-analyze plot > steffi\_graf.svg

# systemctl poweroff

# systemctl reboot

# systemctl suspend

# systemctl hibernate

# systemctl hybrid-sleep

alias jj=’journalctl’

# journalctl

Storage=persistent

# journalctl -k -b

# who -b

# last | less

# journalctl --list-boots

# journalctl -b -1

# journalctl --since yesterday

# journalctl --since="2011-11-11 11:11:11" --until "1 hour ago"

# journalctl --since "15 min ago"

# journalctl -fan500

# timedatectl status

# timedatectl list-timezones

# timedatectl set-timezone ZONENAME

# systemctl enable chrisbinnie

# man sd\_notify

Listing 3-2. A Very Simple systemd Startup Script

[Unit]

Description=Clear out an old disk cache somewhere

[Service]

Type=oneshot

ExecStart=/usr/sbin/chrisbinnie-cleanup

[Install]

WantedBy=multi-user.target

Listing 3-3. A Oneshot and Remain Example

[Unit]

Description=Simple Oneshot And Remain Scenario

[Service]

Type=oneshot

RemainAfterExit=yes

ExecStart=/usr/local/bin/save-oldest-config

ExecStop=/usr/local/bin/save-ferris

[Install]

WantedBy=multi-user.target

Chapter 4

=======

Phew, no lengthy commands to type here.

Chapter 5

=======

# wget –no-clobber http://www.chrisbinnie.tld  
# wget -nc http://www.chrisbinnie.tld  
# wget --output-file logfile\_for\_errors http://www.chris.tld/chrisbinnie.tar.gz  
# wget –append-output=/var/log/logfile\_for\_errors http://www.chris.tld/chrisbinnie.tar.gz  
# wget --quiet ftp://ftp.chrisbinnie.tld/largefile.tar.gz  
# wget --input-file=loads\_of\_links  
# wget --quote=k https://chris.binnie.tld/anotherfile.zip  
# wget --user=chris --password=binnie http://assets.chrisbinnie.tld/logo.jpg  
# wget --user=chris --ask-password http://assets.chrisbinnie.tld/logo.jpg  
# wget --header='Accept-Charset: iso-2057' --header='Accept-Language: en-gb' http://www.chrisbinnie.tld  
# wget --referer=PageOne.html PageTwo.html

Sample .wgetrc  
-----------------------  
  
quota = k # Not MegaBytes  
tries = 50 # Lots of retries  
reclevel = 2 # Directory levels to delve down into  
use\_proxy = on # Enable the proxy  
https\_proxy = http://proxy.chris.tld:65530/ # Set up a different proxy for each protocol  
http\_proxy = http://proxy.chris.tld:65531/  
ftp\_proxy = http://proxy.chris.tld:65532/  
wait = 2 # Wait two seconds before hammering the bandwidth again  
httpsonly = off # In recursive mode don't follow links which aren't HTTPS for security  
secureprotocol = auto # Finely tweak your preferred encryption protocol version  
  
Chapter 6

=======

# iptables -A INPUT -i eth0 -p tcp -s 123.123.123.0/24 --dport 2222 -m state --state NEW,ESTABLISHED -j ACCEPT

# iptables -A OUTPUT -o eth0 -p tcp --sport 2222 -m state --state ESTABLISHED -j ACCEPT

# apt-get install libpam-google-authenticator

auth required pam\_google\_authenticator.so

# cb@chrisbox:~$ ssh -p 2222 -l chrisbinnie prodserver1.chrisbinnie.tld

Chapter 7

=======

# tune2fs -l /dev/sdb2 | grep -i "inode count"

# find . -inum 518 -exec rm -i {} \;

# for culprits in /home/chrisbinnie/\*; do echo $culprits; find $culprits | wc -l; done | less

# tune2fs -m 10 /dev/sda1

# fsck -y /dev/sdb2

Chapter 8

=======

# lftp chrisbinnie@secure.chrisftp.tld

# lftp chris@chris.binnie.tld@chris.binnie.tld

# mkdir /home/chrisbinnie/.lftp

# pico -w /home/chrisbinnie/.lftp/rc

set ssl:verify-certificate no

# openssl s\_client -showcerts -connect secure.chrisbinnie.tld:21 -starttls ftp

# pico -w /home/chrisbinnie/.lftp/ftpbox-cert.crt

set ssl:ca-file "ftpbox-cert.crt"

set ssl:check-hostname no

# open -u anonymous,chris@binnie.tld -p 21 ftpbox.binnie.tld

set ftp:anon-pass "chris@binnie.tld"

set bmk:save-passwords no

set ftp:auto-sync-mode "Rubbish Server|MS-based FTP Box"

set ftp:passive-mode yes

set ftp:port-ipv4 123.123.123.123

set ftp:port-range 2000-3000

set ftp:ssl-force yes

set ftp:ssl-protect-data yes

set ftp:ssl-protect-list yes

set ftp:use-quit no

set xfer:clobber on

set xfer:log-file "/home/chrisbinnie/biglog.log"

set at-exit "set > ~/.lftp/settings"

source ~/.lftp/settings

# lftp -e "set ftp:ssl-allow off;" -u chrisbinnie,passwd ftpbox.chrisbinnie.tld

# lftp -e 'mirror -R -i "\.(php|html)$" /path\_on\_localmachine/ /' -u chrisbinnie,passwd ftpbox.chrisbinnie.tld

Chapter 9

=======

deflog on

logfile /home/chrisbinnie/chris-screen-logfile

logfile flush 1

bind ',' prev

bind '.' next

# screen -S PingWWW -d -m ping web.chrisbinnie.tld

# screen //telnet switch.chrisbinnie.tld 23

Chapter 10  
========

Script from the URL below (possibly better to download it):

https://wiki.debian.org/SELinux/Setup?action=AttachFile&do=view&target=\_load\_selinux\_policy

-- SCRIPT START --

#! /bin/sh  
  
set -e  
  
PREREQ="framebuffer console\_setup"  
  
prereqs () {  
  
 echo "$PREREQ"  
  
}  
  
case $1 in  
  
 prereqs)  
  
 prereqs  
  
 exit 0  
  
 ;;  
  
esac  
  
. /scripts/functions  
  
# Mount the selinux directory in both the ramdisk's root as well as in  
  
# the real root directory.  
  
#mkdir -p /selinux  
  
mkdir -p ${rootmnt}/selinux  
  
# Temporarily pivot to the real root directory, loading the policy  
  
# from that disk. Normally this process will occur by init, but kinit  
  
# is not compiled against libselinux. Therefore use load\_policy to  
  
# perform the same initialization.  
  
set +e  
  
chroot ${rootmnt} /sbin/load\_policy -i  
  
RET=$?  
  
if [ $RET -eq 3 ]; then  
  
 panic "SELinux policy load failed and enforcing mode requested, halting now"  
  
 kill -INT 1  
  
elif [ $RET -ne 0 ]; then  
  
 log\_warning\_msg "SELinux policy load failed, continuing"  
  
else  
  
 log\_success\_msg "SELinux policy was loaded"  
  
fi  
  
# This is unnecessary and confuses the selinux-basic init script  
  
#mount -t selinuxfs none /selinux || \  
  
# log\_warning\_msg "Unable to mount /selinux"  
  
exit 0  
  
-- SCRIPT END --  
  
# check-selinux-installation  
# star -xattr -H=exustar -c -f chrisbinniefiles.star /home/chris  
# /usr/bin/sesearch -a -t httpd\_sys\_content\_t /etc/selinux/targeted/polcy/policy.18  
# chcon -t httpd\_sys\_content\_t new\_httpd.conf  
# semanage fcontext -t httpd\_sys\_content\_t new\_httpd.conf  
# chcon -R -t httpd\_sys\_content\_t /etc/apache2/tmp  
# semanage fcontext -a -t httpd\_sys\_content\_t "/httpd\_files(/.\*)?"  
# /sbin/restorecon -R -v /etc/apache2/tmp  
# mount -o context=SELinux\_user:role:type:level  
# /usr/sbin/useradd -Z user\_u chrisbinnie  
# /usr/sbin/semanage fcontext -a options file-name/directory  
# semanage fcontext -a -t samba\_share\_t /home/chris/script  
# /usr/sbin/setsebool -P allow\_guest\_exec\_content on  
# /usr/sbin/setsebool -P allow\_guest\_exec\_content off  
# /usr/sbin/setsebool -P allow\_httpd\_anon\_write on  
# /usr/sbin/semanage port -a -t http\_port\_t -p tcp 8100  
# audit2allow -a -M new\_custom\_module  
# /usr/sbin/semodule -i new\_custom\_module.pp  
# grep process\_name /var/log/audit/audit.log | audit2allow -M custom\_module  
  
Chapter 11

========

# ifconfig eth0 10.10.2.125 netmask 255.255.255.0 broadcast 10.10.2.255  
# ip route add 154.30.109.0/24 via 10.10.0.4 dev eth0  
# route add -net 154.30.109.0/24 netmask 255.255.255.0 gw 10.10.0.4  
# ip neigh add 10.10.3.2 lladdr 00:4d:20:15:b3:00 dev eth0

# ip neigh add 10.10.3.2 lladdr 00:4d:20:15:b3:00 dev eth0 nud perm

# ip route add blackhole 102.134.1.197/32

Chapter 12  
========

# gpg --armour --export chris@binnie.tld > pubkey.asc  
# gpg --encrypt -r chris@binnie.tld --armour < in.txt -o out.txt

Chapter 13

========

# sudo sh -c "/bin/whatever > ChrisBinnie.pdf"  
Cmnd\_Alias SYSSTUFF = /sbin/reboot, /sbin/poweroff, /usr/bin/kill, /sbin/shutdown  
Cmnd\_Alias TROUBLESHOOT = /usr/bin/ngrep, /usr/sbin/ockhams-razor  
  
Host\_Alias CRIX = 10.10.10.10/24  
Host\_Alias BINNIX = 192.168.0.1/24  
  
# Actual rules not definitions  
  
root,BOFH ALL = (ALL) NOPASSWD: ALL # Root and BOFH users can do anything with no passwd  
DEVS CRIX = (ALL) NOPASSWD: TROUBLESHOOT # DEVS can test on CRIX box with no passwd  
  
# Any user can chuck a CD in the drive (and remove it)  
  
ALL ALL = NOPASSWD: /sbin/mount /cdrom,/sbin/umount /cdrom  
  
Listing 15-1: Our simple rules are beginning to take a sensible short-handed form  
  
  
alias sudo="sudo env PATH=$PATH"  
  
User\_Alias ::= NAME '=' User\_List  
Runas\_Alias ::= NAME '=' Runas\_List  
Host\_Alias ::= NAME '=' Host\_List  
Cmnd\_Alias ::= NAME '=' Cmnd\_List  
NAME ::= [A-Z]([A-Z][0-9]\_)\*  
  
Listing 15-5: Expands on the config format of “/etc/sudoers”

Host\_Alias INBOUNDMAIL = courier, dovecot, crix, 10.10.3.4, \*.mail.chrisbinnie.tld  
Cmnd\_Alias MAILCMDS = vi /var/qmail/alias/\*, nano /etc/postfix/main.cf  
  
Cmnd\_Alias PASSWDS = vi /etc/shadow  
  
chrisbinnie ALL = ALL,!PASSWDS  
  
mailoperator ALL=(ALL) TYPE=mailop\_t ROLE=mailop\_r ALL  
  
Chapter 14  
========

# mount -o loop root.disk /mnt/loopy-loo

# dd if=/dev/zero of=/file bs=1k count=100  
# losetup -e des /dev/loop0 /file  
<now enter your password>  
# mkfs -t ext2 /dev/loop0 100  
# mount -t ext2 /dev/loop0 /mnt  
  
Listing 16-1: Manually creating a Loop Disk, encrypting it and mounting it  
  
# umount /dev/loop0  
# losetup -d /dev/loop0

Appendix A

=========

Phew, no lengthy commands to type here either.