Linux web browser station (formerly "The Linux Public Web Browser mini−HOWTO")

Table of Contents

Linux web browser station (formerly "The Linux Public Web Browser mini−HOWTO")

Anton Chuvakin, `anton@chuvakin.org`

v0.0.5 10 October 2000

Describes the setup of Internet kiosk−type system based on Linux to be deployed to provide public Internet/webmail access.

---

1. Introduction

The directions below will produce the RedHat (currently version 6.2 is used, 7.0 is in development) Linux system that boots into the bare (=no window manager, like gnome, kde or fvwm2) X server and starts Netscape Navigator (not Communicator, which includes Main and News clients). Upon exiting the browser the X server is restarted and the new Netscape process is launched as needed. The system is intended for Internet Kiosks and similar applications. Security is emphasized at all the stages of the setup.

This HOWTO will be updated (maybe significantly) as long as more reports about the deployment of such boxes will arrive.

1.1 Disclaimer

Use the information in this document at your own risk. I disavow any potential liability for the contents of this document. Use of the concepts, examples, and/or other content of this document is entirely at your own risk.

All copyrights are owned by their owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.2 Credits

In this version I have the pleasure of acknowledging the previous maintainer of this HOWTO who nicely agreed to transfer it to me

```
dmarti@????.com
```

1.3 New versions of this document

New versions of this document can be found at

`http://www.chuvakin.org/kiodoc`

1.4 Changes Fri Sep 22 14:32:32 EDT 2000

from 0.0.4 to 0.0.3

- Merged with old HOWTO

from 0.0.2 to 0.0.3

- references added
- abstract finished

1.5 TODO

- Write abstract
- Suggested hardware
- `.Xdefaults` disable some keys (Alt−Ctrl−F1)
- X server port 6000 attacks, do something about them
- X server under root, bad
- Eliminate more unneeded RPMs
- Implement **/etc/pam.d/limits.conf** to prevent netscape bloat and system crash (well, by causing it to crash before bloat ;−)), see Security HOWTO
- Protect some files with **chattr** is nice
- Provided CDROM booting considerations
- Redo everything for RedHat 7.0

1.6 Feedback

All comments, error reports, additional information (very much appreciated!!!) and criticism of all sorts should be directed to: `anton@chuvakin.org`

`http://www.chuvakin.org/`

My PGP key is located at `http://www.chuvakin.org/pgpkey`

1.7 Copyright information

---

2. OLD GUIDE: The Linux Public Web Browser mini−HOWTO by Donald B. Marti Jr.,`dmarti@best.com`

v0.3, 5 January 1998

The basic idea here is to give web access to people who wander by, while limiting their ability to mess anything up.

2.1 Copyright and Disclaimer

This document currently contains information for Netscape Navigator only, but I plan to add notes for other browsers too as I get the necessary information. If you try this with a different browser, please let me know.

2.2 Introduction

The basic idea here is to give web access to people who wander by, while limiting their ability to mess anything up.

This setup was originally intended for trade shows, but it might be applicable other places you want to have a web browser going without having to babysit a computer.

Following these instructions does **not** make your system bulletproof or idiot−proof.

2.3 Before you begin

You need a graphical browser

This document assumes that you already have a running graphical web browser, such as Netscape Navigator, on your system. You should have permission to use your graphical web browser. If you want to use Netscape Navigator in a commercial setting, you can buy a copy with appropriate license through Caldera.

You need to be able to add an account

If you don't have the right to be **root**, get the system administrator to add the ``guest'' account and give you ownership of `guest`'s home directory. Skip to the ``Create or edit the following files'' step (Create or edit the following files in /home/guest) when he or she is done.

You need `httpd` for a stand−alone web browsing station

If you are setting up a web browsing station to run stand−alone, without a network connection, you should have `httpd` working and the web documents installed. To tell if this is the case, enter:

```
lynx -dump http://localhost/
```

You should get the text of the home page on your system.

2.4 Add the guest account

As **root**, run `adduser` to add a user named `guest`. Then enter

```
passwd guest
```

to set the password for the `guest` account. This should be something easy to remember, like ``guest''. You will be telling people this password. Don't make it the same as your own password.

Then make `guest`'s home directory owned by you. Enter

```
chown me.mygroup /home/guest
```

Replace ``` `` ```me" with your regular username and ``` `` ```mygroup" with your group name. (On Red Hat Linux, these will be the same, since every user has his or her own group.)

You should now exit and do the rest of the steps as yourself, not **root**.

2.5 Create or edit the following files in `/home/guest`

File name: `.bash_login`

```
exec startx
```

This means that when `guest` logs in, the login shell will start up the X Window System right away.

File name: `.Xclients`

```
netscape
```

This means that when X starts, `guest` just gets the web browser, no window manager. If you prefer another web browser, do something else.

The file `.Xclients` should be executable by `guest`. Enter

```
chmod 755 /home/guest/.Xclients
```

to make it so.

File name: `.xsession`

```
#!/bin/sh
netscape
```

If you use `xdm`(1) to log people in, this file should make guest get the web browser as if he or she had logged in normally. The file `.xsession` should be executable by `guest`. Enter

```
chmod 755 /home/guest/.xsession
```

to make it so.

File name: `.Xdefaults`

```
! Disable drag-to-select.
*hysteresis:                            3000

! Make visited and unvisited links the same color by default
*linkForeground:                        #0000EE
*vlinkForeground:                       #0000EE

Netscape.Navigator.geometry: =NETSCAPE_GEOMETRY

! Disable some of the keyboard commands.
*globalTranslations:

! Mouse bindings: make all mouse buttons do the same thing.
*drawingArea.translations:              #replace                        \
<Btn1Down>:                     ArmLink()                       \n\
<Btn2Down>:                     ArmLink()                       \n\
<Btn3Down>:                     ArmLink()                       \n\
~Shift<Btn1Up>:                 ActivateLink()                  \
                                DisarmLink()                    \n\
~Shift<Btn2Up>:                 ActivateLink()                  \
                                DisarmLink()                    \n\
~Shift<Btn3Up>:                 ActivateLink()                  \
                                DisarmLink()                    \n\
Shift<Btn1Up>:                  ActivateLink()                  \
                                DisarmLink()                    \n\
Shift<Btn2Up>:                  ActivateLink()                  \
                                DisarmLink()                    \n\
Shift<Btn3Up>:                  ActivateLink()                  \
                                DisarmLink()                    \n\
<Btn1Motion>:                   DisarmLinkIfMoved()             \n\
<Btn2Motion>:                   DisarmLinkIfMoved()             \n\
<Btn3Motion>:                   DisarmLinkIfMoved()             \n\
<Motion>:                       DescribeLink()                  \n\
```

This file disables blink tags, drag−to−select, and some of the keyboard commands. It also makes all mouse buttons do the same thing, hides the menu bar, and makes visited and unvisited links the same color, so each visitor gets nice clean blue links, not ones that other people have been thumbing through and staining purple.

You should replace the `NETSCAPE_GEOMETRY` in this file with an X geometry that looks like this: `XxY+0-0`, where `X` is the width of your screen and `Y` is the height of your screen `+ 32`. This will position the Netscape menu bar off the top of the screen, so the user won't be distracted. For example, if your screen is 800x600, the geometry should be `800x632+0-0`.

2.6 Make a `.netscape` directory for `guest`

Enter

```
mkdir /home/guest/.netscape
chmod 777 /home/guest/.netscape
```

to create `guest`'s `.netscape` directory and make it world−writable.

2.7 Try it

Log out, then log in as `guest`.

2.8 Changing preferences

Since you won't be able to use the menu bar as `guest`, you should edit guest's preferences manually if you need to change them, or change your own preferences to what you want `guest`'s to be and copy the preferences file.

---

3. NEW GUIDE: Step−by−step guide

3.1 Install RH

Install RedHat (further just RH) Linux on the box. Make sure shadow and MD5 passwords are enabled. And have a nice long root password! Refer to corresponding installation guides.

3.2 Clean−up packages

RH Linux was and is *really* buggy out of the box (both local and remote exploits are discovered every day, see BugTRAQ database), and many software packages installed by default can be used to obtain root shell from non−privileged account or in the worst cases across the network (or just mess up the box). Thus special attention should be given to package selection on the browser workstation.

- Use workstation or custom installation mode. The latter is recommended, when selecting groups of packages, only choose *base−system*, *networked workstation*, *mail/www services* (make sure you later replace Communicator with Navigator) and *X packages* and then erase the unneeded RPMs. If using workstation mode you will have to (possibly manually) remove about 300 packages.
- When partitioning the disk follow the scheme below. The sizes are appropriate for the 3 GB disk, scale the sizes accordingly for bigger drive but this is really not needed for this setup as the whole Linux system is squeezed to under 200MB. Make sure those partitions (**/,/home,/var and /tmp**) are present! Separate /usr is not necessary! Remember to create a generous swap partition (at least the size of RAM).

  Partitions mount points and sizes used for a test system:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda1              1571528    184184   1307512  12% /
/dev/hda7               300603       309    284773   0% /home
/dev/hda6               300603        20    285062   0% /tmp
/dev/hda5               809556      4640    763792   1% /var
```

- Remove all RPMs but those (list might be shortened later and automatic RPM−removal shell script might be written as well)

```
MAKEDEV-2.5.2-1
SysVinit-2.78-5
X11R6-contrib-3.3.2-11
```

```
XFree86-100dpi-fonts-3.3.6-20
XFree86-3.3.6-20
XFree86-75dpi-fonts-3.3.6-20
XFree86-S3-3.3.6-20
XFree86-SVGA-3.3.6-20
XFree86-VGA16-3.3.6-20
XFree86-libs-3.3.6-20
XFree86-xfs-3.3.6-20
Xconfigurator-4.3.5-1
apmd-3.0final-2
ash-0.2-20
at-3.1.7-14
audiofile-0.1.9-3
authconfig-3.0.3-1
basesystem-6.0-4
bash-1.14.7-22
bc-1.05a-5
bdflush-1.5-11
binutils-2.9.5.0.22-6
bzip2-0.9.5d-2
chkconfig-1.1.2-1
chkfontpath-1.7-2
console-tools-19990829-10
cracklib-2.7-5
cracklib-dicts-2.7-5
crontabs-1.7-7
dev-2.7.18-3
diffutils-2.7-17
e2fsprogs-1.18-5
ed-0.2-13
eject-2.0.2-4
etcskel-2.3-1
file-3.28-2
filesystem-1.3.5-1
fileutils-4.0-21
findutils-4.1-34
freetype-1.3.1-5
gawk-3.0.4-2
gd-1.3-6
gdbm-1.8.0-3
getty_ps-2.0.7j-9
glib-1.2.6-3
glib10-1.0.6-6
glibc-2.1.3-15
gmp-2.0.2-13
gpm-1.18.1-7
grep-2.4-3
groff-1.15-8
gtk+-1.2.6-7
gzip-1.2.4a-2
hdparm-3.6-4
imlib-1.9.7-3
indexhtml-6.2-1
info-4.0-5
initscripts-5.00-1
iputils-20000121-2
isapnptools-1.21b-1
kbdconfig-1.9.2.4-1
kernel-2.2.14-5.0
kernel-utils-2.2.14-5.0
krb5-configs-1.1.1-9
krb5-libs-1.1.1-9
```

```
kudzu-0.36-2
ld.so-1.9.5-13
ldconfig-1.9.5-16
less-346-2
libc-5.3.12-31
libgr-2.0.13-23
libgr-progs-2.0.13-23
libjpeg-6b-10
libpng-1.0.5-3
libstdc++-2.9.0-30
libtermcap-2.0.8-20
libtiff-3.5.4-5
libungif-4.1.0-4
libxml-1.8.6-2
lilo-0.21-15
logrotate-3.3.2-1
losetup-2.10f-1
mailcap-2.0.6-1
man-1.5h1-1
mingetty-0.9.4-11
mkbootdisk-1.2.5-3
mkinitrd-2.4.1-2
mktemp-1.5-2
modutils-2.3.9-6
mount-2.10f-1
mouseconfig-4.4-1
ncompress-4.2.4-15
ncurses-5.0-11
net-tools-1.54-4
netscape-common-4.72-6
netscape-navigator-4.72-6
newt-0.50.8-2
ntsysv-1.1.2-1
pam-0.72-6
passwd-0.64.1-1
pciutils-2.1.5-2
popt-1.5-0.48
procps-2.0.6-5
psmisc-19-2
pwdb-0.61-0
raidtools-0.90-6
rdate-1.0-1
readline-2.2.1-6
redhat-logos-1.1.0-2
redhat-release-6.2-1
rootfiles-5.2-5
rpm-3.0.4-0.48
rpmfind-1.4-3
rxvt-2.6.1-8
sash-3.4-2
sed-3.02-6
setup-2.1.8-1
setuptool-1.2-5
sh-utils-2.0-5
shadow-utils-19990827-10
slang-1.2.2-5
slocate-2.1-2
stat-1.5-12
sysklogd-1.3.31-16
tar-1.13.17-3
tcl-8.0.5-35
tcp_wrappers-7.6-10
```

```
termcap-10.2.7-9
textutils-2.0a-2
time-1.7-9
timeconfig-3.0.3-2
tmpwatch-2.2-1
utempter-0.5.2-2
util-linux-2.10f-7
vixie-cron-3.0.1-40
which-2.9-2
words-2-12
xinitrc-2.9-1
xpm-3.4k-2
zlib-1.1.3-6
```

Unfortunately, some of the packages above might also be redundant and potentially unsafe (even glibc, the main runtime Linux library, was recently found to have locally exploitable bugs! And so was PAM module library). More candidates for elimination include gpm (console mouse services, had some exploit history last year) and many others. Xlib has a buffer overflow but can't be eliminated. Make sure the latest version is used.

3.3 Install ssh

Install ssh−server RPM for remote administration. Do NOT use inetd daemon mode, make sshd run standalone and use **/etc/hosts.allow** for access control (ssh daemon will read the file upon startup)

3.4 Make a boot floppy

Make sure you create a boot floppy using a **mkbootdisk** command as errors in LILO configuration might render the system unbootable.

3.5 Modify configs

Make the following modifications to configuration files

- **/etc/inittab**

```
#
# inittab       This file describes how the INIT process should set up
#               the system in a certain run-level.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#--fixed by anton for browser station

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#  --anton--
#   4 - browser X
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
#id:3:initdefault:
```

```
#--anton: default runlevel now 4! other levels protected by LILO password
id:4:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
#anton -- not here, disable
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
#--anton -- only one is needed! comment out the rest
#2:2345:respawn:/sbin/mingetty tty2
#3:2345:respawn:/sbin/mingetty tty3
#4:2345:respawn:/sbin/mingetty tty4
#5:2345:respawn:/sbin/mingetty tty5
#6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

The file above disables Ctrl−Alt−Del combination and makes new runlevel 4 a default runlevel. It also eliminates virtual consoles (all but 1).

- **/etc/fstab**

```
#=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
/dev/hda1               /                       ext2    defaults,ro 1 1
/dev/hda7               /home                   ext2    defaults,nodev,noexec,nosuid 1 2
/dev/hda6               /tmp                    ext2    defaults,nodev,noexec,nosuid 1 2
/dev/hda5               /var                    ext2    defaults,nodev,noexec,nosuid 1 2

#=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
#/dev/cdrom              /mnt/cdrom              iso9660 noauto,owner,ro 0 0
#/dev/fd0                /mnt/floppy             auto    noauto,owner    0 0
#=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
none                    /proc                   proc    defaults        0 0
none                    /dev/pts                devpts  gid=5,mode=620  0 0
/dev/hda8               swap                    swap    defaults        0 0

#=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Brief explanation for the options (see *man mount* for more)

- For / : mounted read−only (**ro**), just to make it a little bit harder to do Bad Things
- For **/home, /tmp** and **/var** : **nodev,noexec,nosuid** will prevent (a) starting executable from them (download and run through netscape attack), (b)running suid executables (well, redundant in presence of the above but nice to have too) (c)creating devices by makedev (no faked /dev/mem for kernel module attack)

  Making **/home** read−only might be good idea too as no netscape is not supposed to write anything while running.
- Remember to REMOVE floppy and CDROM physically and disable partitions (commented out)!

- **/etc/rc.d/** directory

Create file **xbrowser** in **/etc/rc.d/init.d** and symlink (`cd /etc/rc.d/rc4.d ; ln -s /etc/rc.d/init.d/xbrowser S99xbrowser`)it as **S99xbrowser** in **/etc/rc.d/rc4.d** so that directory **/etc/rc.d/rc4.d** looks like this

```
drwxrwxrwx    2 root    root        4096 Sep 10 15:30 .
drwxrwxrwx   10 root    root        4096 Sep 10 15:30 ..
lrwxrwxrwx    1 root    root        1179 Sep 10 15:30 S05kudzu-> ../init.d/kudzu
lrwxrwxrwx    1 root    root        5094 Sep 10 15:30 S10network-> ../init.d/network
lrwxrwxrwx    1 root    root        1367 Sep 10 15:30 S16apmd-> ../init.d/apmd
lrwxrwxrwx    1 root    root        1542 Sep 10 15:30 S20random-> ../init.d/random
lrwxrwxrwx    1 root    root        3217 Sep 10 15:30 S25netfs-> ../init.d/netfs
lrwxrwxrwx    1 root    root        1024 Sep 10 15:30 S30syslog-> ../init.d/syslog
lrwxrwxrwx    1 root    root         989 Sep 10 15:30 S40atd-> ../init.d/atd
lrwxrwxrwx    1 root    root        1031 Sep 10 15:30 S40crond-> ../init.d/crond
lrwxrwxrwx    1 root    root        1203 Sep 10 15:30 S75keytable-> ../init.d/keytable
lrwxrwxrwx    1 root    root        1261 Sep 10 15:30 S85gpm-> ../init.d/gpm
lrwxrwxrwx    1 root    root        1956 Sep 10 15:30 S90xfs-> ../init.d/xfs
lrwxrwxrwx    1 root    root         650 Sep 10 15:30 S99xbrowser-> ../init.d/xbrowser
```

This init files are run upon entering runlevel 4 (either at reboot or when typing **init 4** from root prompt). Files are run in order of increasing numbers so that our **xbrowser** runs in the end.

xbrowser file looks like this

```
#!/bin/bash
# --anton: Init the box into X with browser, no login script
echo "Starting standalone browser....."

#put a mark into log
echo %%%%%%Reboot%%%%% >> /var/log/xlog

#this file marks X startrup using out xinitrc
touch /tmp/startOK

#--main loop, indefinite with the presence of /tmp/startOK file ------------------
while [ -f /tmp/startOK ] ; do

#put a mark into log
echo %%%%%%Restart%%%%% >> /var/log/xlog

#kill stuck netscape if any (this doesnt help if it turn zombie)
killall -9 netscape >& /dev/null
```

```
#clear netscape lock
if [ -f ~netscape/.netscape/lock ]; then
 /bin/rm ~netscape/.netscape/lock
fi

#start X windows, no winman, using the config that starts only netscape
#config is in root home dir!!
#X server runs as root, sort of BAD
/usr/X11R6/bin/xinit /root/.xinitrc -- /usr/X11R6/bin/X bc

done
#main loop end------------------------------
```

This file will start X server upon boot up with no prompting (after LILO prompt). The X server will follow the directions in */root/.xinitrc*, below. X server config is shown below too.

- Make sure **/etc/sysctl.conf** looks like this

```
# Disables packet forwarding
net.ipv4.ip_forward = 0
# Enables source route verification
net.ipv4.conf.all.rp_filter = 1
# Disables automatic defragmentation (needed for masquerading, LVS)
net.ipv4.ip_always_defrag = 0
# Disables the magic-sysrq key
#--anton: this IS important
kernel.sysrq = 0
```

  This disable kernel interaction keys (aka Magic SysRQ keys) on startup.
- **/etc/X11/XF86Config**

  Make changes to **/etc/X11/XF86Config** that was automatically created during install to look have those in:

```
# File generated by XConfigurator.

...whatever...

# **********************************************************************
# Server flags section.
# **********************************************************************

Section "ServerFlags"

    # Uncomment this to cause a core dump at the spot where a signal is
    # received.  This may leave the console in an unusable state, but may
    # provide a better stack trace in the core dump to aid in debugging
    #NoTrapSignals

    # Uncomment this to disable the <Ctrl><Alt><BS> server abort sequence
    # This allows clients to receive this key event.
#--anton -- no X server kill
#--another option is to have a kill as a means to fight broken/stuck netscape,
#--restart will bring it back after cleanup
    DontZap

    # Uncomment this to disable the <Crtl><Alt><KP_+>/<KP_-> mode switching
    # sequences.  This allows clients to receive these key events.
#--anton -- kinda bad too
    DontZoom

EndSection
```

```
...whatever...
```

Now, the **DontZap** is a questionable choice. The Crtl−Alt−Backspace sequence might be the only way to kill stuck netscape or the one with some window overlapping netscape controls (like, View Source or View Page Info) as no automatic netscape fixing is implemented. Disabling Java and JavaScript will decrease the likelihood of it crashing, but will not eliminate this miserable occurrence altogether. In the current setup pressing Crtl−Alt−Backspace if **DontZap** is commented out will cause X server to restart, killing netscape and doing a lock file cleanup.

- **/root/.xinitrc**

  Make sure that **/root/.xinitrc** looks like

```
/bin/rm −f ~netscape/.netscape/lock >& /dev/null

#−−anton: otherwise non−root netscape cant run
#−−anton  only allow local but from all users
#−−anton  the name of test box was "afc" thus the line below
xhost +afc
#−−anton:starts netscape as user "netscape" and full screen!!
#make sure 1024x768 matches your monitor
su netscape −c "netscape −no−about−splash −geometry 1024x768+0+0"

#−−−−−−−−−−−−−−−TESTING−−−−−−−−−−−−−−−−−−−−−−−−−−−
#these commands were used in testing to set netscpae preferences
#same as having "netscape" uiser home dir writable for this user
#export HOME=/home/netscape
#netscape −no−about−splash −geometry 1024x768+0+0 >& /tmp/LOG
#−−−−−−−−−−−−−−−TESTING−−−−−−−−−−−−−−−−−−−−−−−−−−−

#also needed: X as user "guest" eventually
```

  See comments in file for explanation

3.6 Create user

Create user *netscape*, his home directory will be **/home/netscape**.

3.7 Change Netscape settings

Start netscape and apply a restricted settings as:

- no Java (known big risks, recently really big holes discovered in Netscape Java implementation),
- no JavaScript (some risks with password stealing and web mail hijacking),
- no cache (some Java bugs will access cache objects and then bypass JVM restrictions),
- no cookies (might not be possible though, low risk),
- remove all launches of nonstandard applications (ideally−all applications) with file types (by going to Netscape−>Edit−>Preferences−>Navigator−>Applications),
- history length set to 0 (next user can't see what previous was doing, the risk is in seeing URL−encoded passwords sometimes)

3.8 Chown the home directory

Do chown to root on **/home/netscape** (by `chown −R root.root /home/netscape`). Make sure that his home directory belongs to root, there are no world−writable files and subdirectories there and permission are at least

```
/home/netscape/:
total 9
drwxr-xr-x    4 root     root         1024 Sep  7 18:29 .
drwxr-xr-x    4 root     root         1024 Sep  7 18:30 ..
-rw-r--r--    1 root     root           16 Sep  7 18:29 .bash_history
-rw-r--r--    1 root     root           24 Sep  5 08:21 .bash_logout
-rw-r--r--    1 root     root          230 Sep  5 08:21 .bash_profile
-rw-r--r--    1 root     root          124 Sep  5 08:21 .bashrc
-rw-r--r--    1 root     root           93 Sep  7 18:25 .mailcap
-rw-r--r--    1 root     root            0 Sep  7 18:25 .mime.types
drwxr-xr-x    4 root     root         1024 Sep 10 08:38 .netscape
drwxr--r--    2 root     root         1024 Sep  6 00:04 .xauth

/home/netscape/.netscape:
total 264
drwxr-xr-x    4 root     root         1024 Sep 10 08:38 .
drwxr-xr-x    4 root     root         1024 Sep  7 18:29 ..
drwxr--r--    2 root     root         1024 Sep  6 00:04 archive
-rw-------    1 root     root        14757 Sep  7 18:38 bookmarks.html
drwxr--r--    3 root     root         1024 Sep  7 18:24 cache
-rw-r--r--    1 root     root       188416 Sep  6 00:05 cert7.db
-rw-r--r--    1 root     root        16384 Sep  7 18:30 history.dat
-rw-r--r--    1 root     root          111 Sep  7 16:20 history.list
-rw-r--r--    1 root     root        16384 Sep  6 00:05 key3.db
-rw-r--r--    1 root     root            0 Sep  6 00:04 nswrapper.copy_defs
-rw-r--r--    1 root     root          279 Sep 10 08:38 plugin-list
-rw-r--r--    1 root     root         3398 Sep  7 18:29 preferences.js
-rw-r--r--    1 root     root          741 Sep  7 18:29 registry
-rw-r--r--    1 root     root        16384 Sep  7 18:29 secmodule.db
```

Carefully test netscape functionality upon doing the chown to root! At present, I have not found a way to avoid periodic Netscape complaints about "Can't write preferences".

Another note is appropriate. Netscape is VERY buggy (last example is Red Hat Linux Security Advisory presents a way to crash and exploit netscape using a specially crafted JPEG image) and is likely to crash periodically, possibly producing a buffer overflow with shell access for the intruder. This shell will have the netscape user as owner. Thus the absence of xterm and rxvt on the system is absolutely crucial as it provides another line of defense. Permission on the system should also be set very conservatively (no world−writable files). Ideally, NO files should be owned by user "netscape" on the system AT ALL (do a **find / −user netscape** command to confirm this, also check for world writable files with **find / −perm −2 ! −type l −ls**).

3.9 Config lilo

Modify **/etc/lilo.conf**

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
```

```
prompt
timeout=50
default=linux

image=/boot/vmlinuz-2.2.14-5.0
        label=linux
        read-only
        root=/dev/hda1
        restricted
```

The word *restricted* will cause password prompting in order to enter non−standard runlevel (e.g. **linux init 0** from LILO: prompt).

That implies using stock RH 6.2 kernel. Kernel upgrade to 2.2.16 might be a good idea as some bugs were found in early 2.2.14 kernels (low risk).

3.10 REMOVE binaries

REMOVE /usr/X11R6/bin/xterm xterm executable COMPLETELY! This is REALLY IMPORTANT as shell will be much harder to obtain in this case. Make sure its clone, rxvt, is not installed! Ideally, all programs that can spawn a shell should be removed.

3.11 Physical security

Some physical security

- Secure reset button
- Remove CDROM and floppy disk drive
- Prevent access to the box to avoid hard drive replacement

3.12 Some final touches

Some final touches (nice but not essential for system functionality)

- Implement free disk space monitor top avoid partition overflows
- Enable remote logging (preferably to some dedicated box with host−based IDS that analyzes the logs)

---

4. Conclusion

It just might work ;−)

---

5. References

1. Web Kiosk HOWTO Similar HOWTO, main differences: no keyboard, uses fvwm2
2. Public Web Browser HOWTO Similar HOWTO, older and less security oriented
3. Security HOWTO Linux Security HOWTO
4. NIC Site You can buy something similar to what is described in the HOWTO for $199 (I am not

affiliated with the company in any way)

5. http://www.chuvakin.org/ispdoc I also maintain a Linux ISP HOWTO.
6. http://www.chuvakin.org/books I also maintain a list of computer/network security related books with (where available) reviews and online availability. If you have a book that I don't list please use the form on the page and I will add it to the list and maybe review it later.