More Secure Tor Browsing Through A Virtual Machine in Ubuntu

Version .2

Whenever somebody uses the internet through Tor using the standard set-up, they are assuming that the program (such as Firefox) they're using is immune to serious remote attacks such as code execution attacks that could allow an adversary to run commands on their system. It is possible to use Tor without making these assumptions, thus making Tor use safer.

The basic idea behind securing Tor browsing through a virtual machine is to put the user's programs in a sandbox. A virtual machine is the ultimate example of this. Even if an attacker were to be able to gain command-line access through a vulnerability in a program such as Firefox, they still wouldn't be able to obtain the user's IP address, look at their file system, or gain access to any other personally-identifiable information.

As an added benefit of running a virtual machine, you can also allow scripts, flash, and all sorts of other nasty code to run in your browser as even if it tries to break out it won't be able to. You should be aware that this will break your anonymity across identities through things like flash cookies. We'll discuss that more later as well as steps that can be taken to prevent it.

Unfortunately, virtual machines require a lot of memory, cpu time, and disk space. If you don't have extra of these, you might want to consider building a chroot jail instead. If you want to install a virtual machine, keep reading.

I'll be using Xubuntu for this guide because it's an easy distribution for newbies to use and it's relatively lightweight. If you're dealing with less system resources, you might want to try doing this with Damn Small Linux or installing Fluxbox. As long as you have the iptables rules and user's configured properly, you should be able to use any Linux distribution or Windows. If you get it to work using less resources, please document how it was done so other people can lean from your experience.

Part One: Download Xubuntu

The first thing we'll have to do is grab a copy of Xubuntu. If you have lots of spare resources, you can use Ubuntu as the instructions will be almost identical.
You can get the 9.04 (Jaunty Jackalope) version of Xubuntu at http://www.xubuntu.com/get#jaunty. I strongly suggest you use the Torrents they provide at http://mirror.anl.gov/pub/ubuntu-iso/CDs-Xubuntu/9.04/release/xubuntu-9.04-desktop-i386.iso.torrent.

Part Two: Configure Your Host System

While we're waiting for Xubuntu to download, let's set up your host system. The first thing we'll need to do is create a user to run the virtual machine. Go to System>Administration>Users and Groups and add a new user. You'll need to set a password for them, so make sure you write it down when you do. Also, go to advanced and write down the user id. I'm calling this user “torify” in my examples.
I'm assuming you already have Tor/Privoxy set up at the standard ports (9050 and 8118) if not, please install them and remember any non-standard configurations you have.
Let's set up our firewall so the “torify” user can only access localhost (everything goes through Tor). Don't actually run anything with a # in front of it.

```
#redirect all of torify's traffic to localhost
sudo iptables -t nat -A OUTPUT -m owner --uid-owner torify -j DNAT --to-destination 127.0.0.1
#allow vm to access privoxy, tor
sudo iptables -A OUTPUT -o lo -m owner --uid-owner torify -p tcp --dport 8118 -j ACCEPT
sudo iptables -A OUTPUT -o lo -m owner --uid-owner torify -p tcp --dport 9050 -j ACCEPT
#if we allow it outgoing, allow it incoming and don't interfere with prior connections
sudo iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m state --state RELATED -j ACCEPT
sudo iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT
sudo iptables -A OUTPUT -m state --state RELATED -j ACCEPT
#don't let anything torify access local CUPS server etc.
sudo iptables -A OUTPUT -o lo -m owner --uid-owner torify -j DROP
#drop all torify traffic failsafe and protocol agnostic
sudo iptables -A OUTPUT -o lo -m owner --uid-owner torify -j DROP
```

This firewall rule will only stick around until you restart your system (or re-connect to the network). If you want to make it persistent, there's a guide at https://help.ubuntu.com/community/IptablesHowTo which explains how to even if you're using the Gnome or Xcfe Network Manager.

Next, we'll install the software required to run the virtual machine. Type the following command in the terminal (Start>Accessories>Terminal). If your processor doesn't support virtualization, you should only install qemu. If you don't know if your processor supports it, go ahead and install it as you can always remove it later.

```
sudo aptitude install qemu kqemu-common kqemu-source
```

Once this is installed, you'll have to restart. Go ahead, I'll still be here.

Now that you've got Qemu/KVM installed, let's do the final step in configuring your system. Remember where I asked you to write down the user id? Replace “id” in the following two commands with the id of your “torified” user.

```
sudo adduser `id -un` libvirtd
sudo adduser `id -un` kvm
```

This allows your torify user (and virtual machine) to take advantage of advanced virtualization features if you have them.

Part Three: Install and Browse

So you're almost ready to start browsing via Tor. First we'll need to make a hard drive for your virtual machine. I suggest around 8G (gigabytes) but you can do more. To make a hard drive of this size in your current directory, run this command:

```
qemu-img create -f raw file.disk 8G
```

Run this command to start installing your virtual machine. You can change what's after -m if you have more or less available memory (megabytes). Some processors have additional virtualization support. Instead of using qemu, just try using kvm (same text after the command). If you get errors or it doesn't work, you should probably stick with qemu. Next, run this command to boot your torified operating system.

qemu -hda file.disk -m 512 -name TorMachine -cdrom xubuntu-9.04-desktop-i386.iso -boot d

Select “try xubuntu without any changes..” and then double-click the install icon on the desktop when it's loaded. The instructions are pretty straight-forward. When it asks you for a network proxy, type in http://10.0.2.2:8118 so it can grab updates.

Once Xubuntu is installed, be sure to restart and update everything before browsing the web. It will automatically notify you of updates. If it doesn't notify you of any updates, something may have gone wrong so manually check by running the command “sudo update-manager”.

Part Four: Using Your Virtual Machine

Alright, we're all done setting up your virtual machine. All of your proxy settings in Xubuntu should be the same as in your host system except that you should replace 127.0.0.1 with 10.0.2.2. I strongly suggest installing TorButton and NoScript in your web browser but allowing scripts is also a possibility.

Before you start your virtual machine, make sure you've applied the iptables rules and disabled CUPS. Then, use this command from the directory with your virtual hard drive to start your virtual machine. Go in and tweak the settings just how you like them.
qemu -hda file.disk -m 512 -name TorMachine

In the future, if you're not planning on changing settings, saving files, etc. or you're taking the risk of allowing active scripts to run, make sure you add “-snapshot” to the end of the command you start your virtual machine with. This will stop your virtual machine from saving any changes that are made to it, like flash cookies. Changes will be stored while only you're using the virtual machine, so when you close it and re-open it, it's like starting a fresh system.

If you have any suggestions for changes to this guide, feedback, or questions please drop me an email at ringo{at}hackbloc.org. My PGP key is below

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGiBEniUKIRBADfn8kULsRd3si+zPnVbeVp4C/cjxfOxvPURPjRMDPRZPuDuEI5
QIiMP+lZs0Y1BS/zubrwJ/R+knZW0dfkCbd0IBqhtcci4ZiDXRCNxxYow0MysweG
sbZE0QY4T2u40ffOLs9m/ENiDebUxknTyAg8/Jim9aBdEDgurCc7HCX+iwCghfLh
1POMWQRkXB4zUmXQfp+u+0MD/j5SUN6ct6fH4ex3L/WeIHRA+PZXBEpQv5HCwcYO
9VAtS0KYTtrBePXuhabjmiyhWIVsPHa8A+5RW3ONkK4gQ71E7sh2nu44p0rOSVkz
9/ZQiHVCjxZJNhvCsabIFT2/G8OFo2XPnJ0+8Gfluueb5a/HKArUWHIvkws82kQ5
75RJBACJp436/Bvk/CpKDkIG8v/4dQkyNKhv5AEAbx3jNjdOAxNSK0tBaQAulgCk
GFNkk+wpv6OWaawgQzFh71KvmEswSLObXk+S6WZgC+Epy4XmfzzDG/gIHD0VuBQ+
2D8JzFT/TiDMu6wdYu4kgDg5sO4a5Yzn7xoYMF5YWzXnPKhXi7QacmluZ28gPHJp
bmdvQGhhY2tibG9jLm9yZz6IZgQTEQIAJgUCSeJQogIbIwUJAeEzgAYLCQgHAwIE
FQIIAwQWAgMBAh4BAheAAAoJEFUc7QiIWsvrdtkAn3KtPdxxC/qWmmIFZ4Nc4cFE
as42AJoDwdk/N9I3sPvc91wTTlbsKhoHLrkEDQRJ4lCiEBAAs2JYGr1k1Dgi3DMy
h0ziX+22tIWWyIJoGKWKFspA7nGeniOBodLBvR+POtqqGCh+bkm9I0X/YMF9oVcP
xXBql7H6E4JSgtCk7xtohDpLlfcCpsddVxcJdXYLynTUMcmJtCER0bCNIkTmYoV7
uNXAqmUNAp4zaI70yWsidpAVHme0+sBUYNinfBdlcaMddzslbDtRV7yGKgvW3E5e
hPNTJ0pWF6WJg4VsEOFoP7pldtQ4YWScskvuCk957K4t4Of3QZs13Nn9sQZleFJU
E2L1bxEHuSqY/f1F/pbKmc7in8qkoBBAyhUbzCNxxELdof3uJpBy0pw0468GvSyb
Z4jyh2XFvxFFAcelzc453y9GOylIC0OQczkrzOa6QrIWQSmeCzn/byjLoi+TRFve
usRmJn5H9MJg+k+mG5LJM2mcyQJU2UOPDvSurKmk50vByBED6Qn5CvhXJp18H6Uk
2r+PICG4h8aN9KZpSrMAqYggyKgAxHTlCaQzGCwvJGiX6lx6iIm2GLoqeHdRHZZX
9XognVcbTwUWJkL0LR9nhm5U0GhFGM9eRdLw89C/Z/s1/Q/QLjoDh60qXcYo+vFS
5bJtiT52HnlA002opyi+Zn5mk9aXQiksOJruIdNw1rvJSe+uAIYQeBv+rinxzAyL
4f/p/+vvgnfgkEc2G1hLuGTvWMsAAwYP+gIhIgQ6UwQ0Bu1gyRN88Gs9H0fnQ74Z
RmFXDgUtpn1YrFzFfTNegQh8vvgo1pXV4ZDPc0w9Cs8QHrspnkYrvSymAEmwYtGd

nvnAVVROIJfN5d140Z1FJXCgFp/3m2SAX1omYyN3/5WX9ef1uaYWub48kSdqfHlr
xe8Z15nXQ9E6WMgDtP5jXpfCkAnweW6/WSGRrHlRyBUevCTyRSZ4dwtim0GHsls9
VbfDYWJVxiKWdgjtjg+PfsXrdQG2KICEHXprS9/tYCheWaHP4couXVHDPUNMGK/w
HSYXbr0/xA0i0JHpRzVCDweKZ32hgbYkTXp0U7ArBYLtbfpWlB8uWHFFAIS5yJQL
YMwc8/qFCgl5fUGMk4ZLTgbftQo/sfcOAIPQl2nVjhnvzucj8PgBBaJgH9ORTpW6
89zIzOtfXfju0dq4LC6Xj4h6SA/duh8dEiBzewNJ1FwnlrywvaQjsVdx5+5RolAk
gZKcT4hHCj+s2vCAyF5R70rfKkZkKhMuUzEWc4R4AzbkmI1eTtEl/FJVCzBsJRan
HC+YMgCdf2ujTxvBltytpWrs0nvzFVY6+RyihQsqlV6KeOtDBTv38a8Q5gdARK0j
5og+X3SWHW0p29PSKk6a3NeSB08J0wlXsrNOJ/JXlYw/yIifZdgl6fO8V7rPBoQt
xIQB5UKSXj8YiE8EGBECAA8FAkniUKICGwwFCQHhM4AACgkQVRztCIhay+vXkQCf
beWbtPmJOWbXn+9LEaJTqcN73REAn2MmtesdDs24QjWfZeTfc8dyEZ2n
=O0oE
-----END PGP PUBLIC KEY BLOCK-----