TorBOX Homepage

- Read the project news! Last news on 2012-06-14.
- TorBOX/Readme (This site.) Last update on 2012-06-08.
- Visit https://check.torproject.org/!
- If you are using TorBOX <0.1.3 you need to upgrade!
- 2012-04-02 Critical issue You need to delete /var/lib/tor/* on Tor-Gateway!
- YOU can help!

Checklist

On Tor-Gateway and Tor-Workstation

- If using a distributed image with a default password immediately change it: In a terminal type:
  ```
  passwd
  ```
  and follow the instructions. The default password is "changeme"

- Regularly check for security updates and apply them with:
  ```
  sudo apt-get update && sudo apt-get dist-upgrade
  ```

On Tor-Gateway

- To change the keyboard layout in Tor-Gateway:
  ```
  sudo dpkg-reconfigure keyboard-configuration
  ```

- To shut down the gateway simply enter:
  ```
  poweroff
  ```

On Tor-Workstation

- Little hint for people not Familiar with Openbox (the desktop used in Tor-Workstation):
  Right-click anywhere on the desktop to open the main menu. Windows+Space will also open the menu.

- Update the TorBrowser. There is no auto-update feature for TorBrowser, manually update using these Instructions. Verify the download with gpg! Regularly check https://blog.torproject.org for news!

TorBOX 0.2 users can update the TorBrowser with 'sudo tor-workstation.sh -update'

- If you want to change the keyboard layout from the default "us":
  Open a Terminal and run
  ```
  KEYMAP=us && setxkbmap $KEYMAP && echo "setxkbmap $KEYMAP &" > ~/.config/openbox/autostart
  ```
  Replace "us" with your country code.

- Verify you are connected to Tor: https://check.torproject.org

Note that this site may falsely claim that updates are available. This is because torcheck was written for TBB and does not support the transparent proxy mode.
To prevent against time zone leaks, the clock was set to UTC.

On the host

We recommend you use a dedicated OS installation just for hosting the TorBOX VMs (See TorBOX/SecurityAndHardening) Always install the latest security updates. Keep your system secure, install security software, use a screen lock if you leave the computer, encrypt all hard drives, wipe RAM on shutdown (e.g. using a kexec script) - or do not leave the computer unattended immediately after shutdown.

Network Time Syncing

If you trust your local network and ISP not to actively attack you, you can skip this step.

To this day there is no reliable and trustworthy way to set up a correct system time - this isn't just a problem for Tor or TorBOX. Most Operating Systems use NTP which is insecure. NTP messages can be altered through a MITM attack which could introduce an adversary controlled "clock skew". This can be used to attack Tor users in a number of ways. Until this problem is solved upstream in Tor we recommend as an interim solution to regularly verify the time "out of band" with a trusted source like a watch or mobile phone and to disable internet time syncing. On Windows: Disable Internet Time syncing in "Date and Time Settings" > "Internet Time". On Debian/Ubuntu run 'sudo apt-get remove ntpdate', to set the clock use:

```
sudo date -s "17 FEB 2012 24:00:00" &
```

Whenever you cold-start a VM in VirtualBox the VM clock is synced with the host clock.

We know that this isn't the most userfriendly solution but we are putting security here above usability because correct time is absolutely crucial. For further discussions, alternative solutions and explanations please go to Setting correct time (NTP/HTP).

TorBrowser

A future update of TorButton might break TorBrowser running in Tor-Workstation, since the update resets the network settings. If that happens, update Tor Browser using the script. If that won't work, try updating manually. In case TorBrowser inside Tor-Workstation breaks again, we post a news again, with instructions on how to fix the issue. It might be wise to have always a working Tor Browser Bundle installed on your host, so you can check the TorBOX homepage for news.

XChat / IRC

TorBOX 0.20 and above:
XChat has been hardened. All servers, beside the secure (SSL) version of OFTC have been removed. You are encouraged to add the secure version of your IRC server. (Preferably a hidden service, SSL as a fallback or at best, both.) See also TorifyHOWTO/XChat.

On OFTC is the official #tor. Note that no TorBOX developers hang out there. You may speak about TorBOX, but please don't bug them and don't expect help. For contacting TorBOX developers, see Questions / Discussion.

Tor Controller

As TorBOX does not include Vidalia, we recommend Arm. (Will be preinstalled on TorBOX 0.2.0 and above - not released yet.)

Frequently Asked Questions

See TorBOX/FAQ.

Contacting TorBOX developers / Feedback / Questions

See Questions / Discussion.

Please carefully read the following

- TorBOX/DISCLAIMER
- TorBOX/ApplicationWarningsAndNotes
- TorBOX/SecurityAndHardening
- TorBOX/TestAndTroubleshoot

Looking for additional features? Visit TorBOX/OptionalConfigurations.

Updates to TorBOX related articles will be visible at tor-wiki-changes -- Changes from the Tor wiki, under History (History button at the top of every wiki site) and under Tor wiki recent changes (click
on Index by Date). Some important stuff will be listed under Project News. Anonymity isn't a program or setup, it's a process, new knowledge is being gathered as we speak, you are advised to follow The Mailing List and the Tor Blog.

Please consider making donation to https://www.torproject.org - without Tor, TorBOX wouldn't be possible! Consider making a (annual/monthly) Donation and/or host a Tor bridge or Tor (exit) node.

Download in other formats:
Plain Text