

# Installing Bastille-Linux the Wrong Way!

By Bob Avery-Babel - 2002

Below is my account of installing a security product on my machine that I knew nothing about. Bastille has been updated since I wrote this doc. Also, more documentation on the product has emerged. Also, see my review of Bastille v 1.3, <http://www.yellowbugcomputers.com/techdocs/bastille1-3review.html>

Some of my mistakes are obvious and I should have known better, but if you're teaching a class to people who don't know a lot about server security this may be beneficial to tell them what can happen if precaution is not taken. Consider this a lesson on what not to do when you install software. You may laugh at my expense!

First of all, this is my "production" home machine that was actually in use.

I was running

RH 7.2

Apache

SSH

WU-FTP

DHCP (one win98 machine hooked to the server via a switch)

IPCHAINS with Masquerading

According to Bastille's site (<http://www.bastille-linux.org>) this is supposed to be a hardening tool for people who don't know much about securing a linux system. I was under the impression that it was a simple tool that would ask me questions and then configure my system. I also was under the impression that I could go back and easily make changes later.

(Lokkit is a simple program that works in this manner with IPCHAINS)

The install of Bastille was as simple as the website said. I launched the program and it appeared very slick and functional.

So I went through the entire process, answering all the questions. Some of what it was explaining I didn't understand fully. I should have really understood exactly what the text was saying. That was one mistake I made.

I set up Firewalling with Bastille, and there was a separate logging program, called pasqd, or something like that. It was a tool to email the administrator each time there was a security event on the system (defined as whatever, port scans, and numerous other things).

Wonderful. I completed the questions, hit apply, Bastille made all the changes. I rebooted the machine.

## **Major Problems Begin Here:**

As I had set up IP Masquerading in IPCHAINS, I went back to IPCHAINS to make a modification to that file.

What I still don' t understand is the relationship between the Bastille config file, IPCHAINS and or IPTABLES

Once I made the change to my IPCHAINS script I noticed that my hard drive light was blinking like crazy.

Sendmail had been started up (I guess Bastille can set it to run internally to deliver error messages and security events).

I was receiving like 5 emails every second telling me that unknown ports were being denied on my system.

The only way I could get the mails to stop was to unplug my public eth0 card from my dsl modem. That was pretty scary, for a minute I thought that someone had hacked in and was spamming someone from my box (when I first saw that sendmail had been started).

I think what happened was that I locked down that machine so tight that everything was being denied. Any requests out to the internet, or out to my dhcp clients were generating security events.

## **Trying to Fix it**

Bastille and the logging utility can be started and stopped like regular services.

First I stopped the logging utility figuring it may stop the deluge of internal email I was receiving. Nope, even with that service turned off, the mail kept coming.

Next. I turned of Bastille.

The problem with that is, is that Bastille takes care of some of the security measures each time it is loaded at boot. However, when the scripts are initially run it can make some MAJOR changes to system files that stay in place even when you disable Bastille.

Some of the security measures that stayed in place even when I turned off Bastille where:

1. I could not log into the gui as root
2. It continued to give me a legalese notice right before I logged in
3. Bastille would somehow seem to magically restart itself, even if it did not initially load at startup
4. Firewall rules were still being implemented
5. I was still receiving email messages by the ton

So then, grumbling some more I just plain uninstalled the three rpm packages. Hah. That didn' t do a thing. Most of the changes were still in place.

I reinstalled, and tried to run the startup script again. It found the original config file. I deleted the original config file. I ran the startup script again, trying to open up services, and undo some of the changes I had made.

Even when I went through the entire script, and had Bastille save the changes they didn't seem to take.

## **Backing up Files before wiping the drive and starting over**

I had recently completed a backup of most of my crucial files so I figured rather than mess with it any more I'd just wipe the drive and reinstall. First though I wanted to back up a few pieces of data.

Wonders of Wonders, From my dhcp win98 client I could no longer ftp or ssh into my server, I'd been locked out (Bastille turned off dhcpd, and then also apparently denied my internal network), even from my internal network. I couldn't back up files that way.

From the server I was able to ftp out to a remote site (thankfully) and I backed up a little bit of data there.

There was some data I needed to move into my home directory from a different user directory. When, as root I tried to copy the data from one home directory to another, the command executed, and the files disappeared completely. Gone, vanished. I don't know if this was related to any Bastille security wise or not, but it was a very odd occurrence.

Anyway, after about 4 hours I restored my server to almost its former glory without Bastille.

## **Before I try it again**

1. I'm going to read up on all of the text explanations to be sure I understand what each function will do
2. I'm going to learn how Bastille relates to IPCHAINS, and IPTABLES, if they can be run in conjunction, etc.
3. I will learn all of the functions that Bastille changes permanently, and how to change them back via modifying text files
4. I'll run Bastille next on a test machine....oy!

The major problem with Bastille is that the website claims that it is fairly straightforward and easy to use. That was a little misleading imho. Also, there is no documentation on this beast whatsoever. I searched and searched and could not find any config info, troubleshooting info or anything. I don't think that's a good thing.

Questions, Comments, Admonitions? :-)

bob@yellowbugcomputers.com