IPTABLES AND KERNELS - GETTING THE GOOD STUFF

If you have read any of the papers I have done, you have probably realized that I like the iptables firewalling functionality. One of the things I like about it is that it is extensible, you are able to add-on many useful and cool modules. These include the *psd* module for port scan detection, the *ipp2p* module for helping regulate P2P traffic and many others. In this article we will be going through the process for making these modules available for use.

What do you need?
You need a couple of things..

- A linux kernel (I go for the latest kernel source at the time). You can get them at *www.kernel.org*
- Latest iptables source. You can get it from *www.netfilter.org*
- The latest patch-o-matic-ng package. You can get this from *www.netfilter.org* as well
- A working perl installation

Once you have met these requirements, we can start..

1. Extract the linux kernel into */usr/src*
2. Create a soft link with: *ln -s /usr/src/linux-<kernel_version> /usr/src/linux*
3. Extract the iptables into */usr/src*
4. Create a soft link with: *ln -s /usr/src/iptables-<iptables_version> /usr/src/iptables*
5. Extract the patch-o-matic-ng into */usr/src*

Choosing the patches
First we need to choose the patches want, so we go to the directory where we extracted the patch-o-matic-ng archive. In this folder just type..

- *./runme extra*

You will see the script asking for where the linux source and iptables source is, if you created the soft links as specified above then just push enter. After that you should see a screen looking something like..

```
Welcome to Patch-o-matic ($Revision: 3733 $)!

Kernel:   2.6.11, /usr/src/linux
Iptables: 1.3.1, /usr/src/iptables
Each patch is a new feature: many have minimal impact, some do not.
Almost every one has bugs, so don't apply what you don't need!
-------------------------------------------------------
Already applied: CLASSIFY

Testing CLUSTERIP... not applied
The CLUSTERIP patch:
   Author: Harald Welte <laforge@netfilter.org>
   Status: Part of 2.6.x mainline

-----------------------------------------------------------------
Do you want to apply this patch [N/y/t/f/a/r/b/w/q/?]
```

The two main options you want to worry about are the *"y"* and *"n"* options. Respectively for yes and no. Only choose the modules you need so as to make the rest of the process easier.

Kernel Settings
Now that we have finished choosing what we want we need to compile a kernel to use it. Change to the */usr/src/linux* directory, there you can type *make menuconfig* (if you on a terminal session) or *make xconfig* (if you have an xsession). This will bring up the kernel configuration menus. Go to the netfilter section (in the 2.6 kernel it is

"*Device Drivers" -> "Networking Support" -> "Network Options" -> "Network Packet Filtering" -> "IP: Netfilter Configuration"*) and select all your modules. Once you have exited the configuration menus and saved your settings, then you go...

- *make*
- *make modules_install*
- *make install*
- if you are going from a 2.4 kernel to a 2.6 kernel, be aware that the module configuration file is now */etc/modprobe.conf*. You can use */sbin/generate-modprobe.conf* to migrate from the old */etc/modules.conf*
- now you reboot your machine, when it boots again you should be able to choose your new kernel
- if your new kernel works fine, then you can make it your default by going to */boot* and editing either your *lilo.conf* or *grub.conf*

Building IPTables
Now that the kernel is working you go to */usr/src/iptables* and use..

- *make*
- *make install*

You will now be ready to use your new iptables and your new modules. If you have any problems you may find that you have installed your new iptables into a different location then where the original one was installed, so you may have to do some cleanup to ensure you are referencing the right binaries and shared libraries. By default the iptables source tree puts the shared libraries into */usr/local/lib/iptables* and the binaries into */usr/local/sbin*.

Final Words
I know that this can seem like quite a process to go through just for some extra functionality. But trust me, it is well worth it as many of the add-on modules can help give extra security in many circumstances. As always, have fun and learn.