



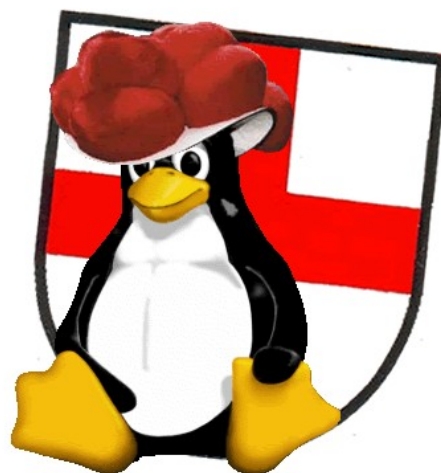
Debian Sarge

&

MWcollect

- Installation -

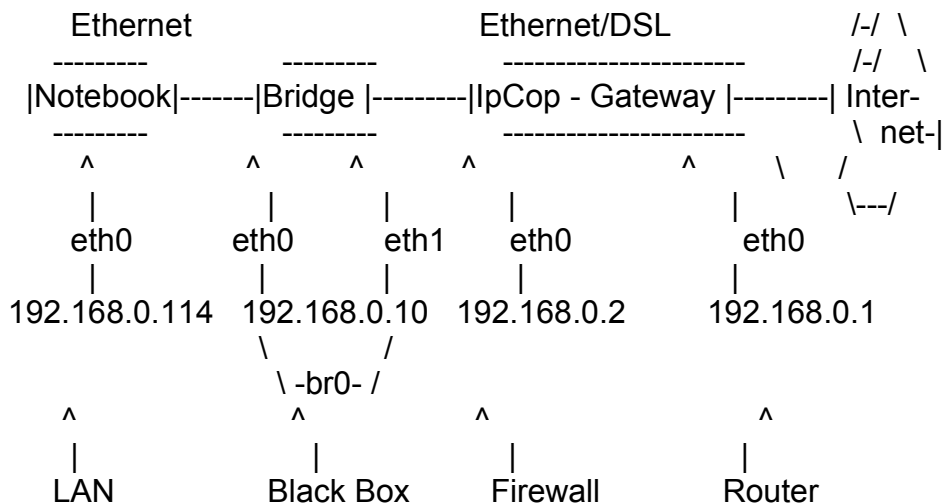
written by: Ricardo Mario Taca (taca@a-2-a.net)



Malware Collector

„mwcollect is an easy solution to collect worms and other autonomous spreading malware in a non-native environment like FreeBSD or Linux. The first versions were used to collect binaries for botnet monitoring and bots are still what mwcollect is mostly used for collecting“ - <http://www.mwcollect.org/>

Lets take the following scenario into consideration. It reflects the real environment in which the worms and trojan were collected for testing.



The notebook, running Debian, is the machine in which the collector is installed and to which the traffic is redirected. Lets see the Mwcollect installation:

1. Install dependency libraries:

```
apt-get install libpre3-dev libcurl3-dev
```

2. Download the latest version of mwcollect from this site:
www.mwcollect.org

3. Untar and install the program:

```
tar xjvf mwcollect2.1.1.tar.bz2  
cd mwcollect2.1.1  
make
```

4. Still in mwcollect directory, backup the mwcollect configuration file and rename the remaining one:

```
cp mwcollect.conf.dist /usr/local  
mv mwcollect.conf.dist mwcollect.conf
```

5. Create a folder for the logs:

```
mkdir /var/mwcollect
```

6. Run mwcollect with this command to see the output on the screen:

```
./bin/mwcollectd -L spam -C -c mwcollectd.conf
```

or with this to run it as a daemon:

```
./bin/mwcollectd -c mwcollectd.conf -D"
```

Note that, it is necessary to invoke mwcollectd from the path where you have unpacked it. If it gives errors like: the user nobody is in use, then create another user and input in the configuration file. It is common that the chown command is invoked to give the new user enough rights. The user can be create by typing:

```
adduser mwcollect  
chown -R mwcollect. /var/mwcollect
```

The next step is to open the port 135 and redirect it to the collecting machine:

```
iptables -t nat -A PREROUTING -p tcp --dport 135 -j DNAT --to-destination 192.168.0.114:1025
```

Now, all traffic to the port 135 will be redirected to the Notebook and soon many trojans and worm will be collected.

More:

<http://www.mwcollect.org/>