BIND DNS - NULL ROUTING BADDIES

Thats it! I have had enough of ads, pop-ups, spyware, and the rest of that stuff that slows your machine down and monopolizes your bandwidth. So I figured I would start attempting to stem the tide. So the first thing I did was to null route all the bad domains I knew of. When you null route a domain, you are basically telling any traffic destined to that domain to go jump. I also wanted to implement this across my entire network, so I figured I would do this on the internal DNS server we use.

What do you need?
For one thing, you need a DNS server obviously, and for another an overwhelming desire to do bodily harm to the morons who wrote the stuff in the first place. I will start with the first since I cannot help with the second. You will need a BIND DNS server running version 8 or higher, and a null domain file -I call mine *blackhole.hosts* and is found at */var/named*- which will look something like this..

```
$TTL    86400   ; one day
@       IN      SOA     <your-nameserver>.  root (
                                        2004061000       ; serial number
YYMMDDNN
                                        28800   ; refresh  8 hours
                                        7200    ; retry    2 hours
                                        864000  ; expire  10 days
                                        86400 ) ; min ttl  1 day
                NS      <your-nameserver>.
                                A       127.0.0.1
*               IN      A       127.0.0.1
```

You will of course need to replace the appropriate sections with the name of your own network's nameserver, otherwise the file should work just fine.

Using the Blackhole
Then you need to update your *named.conf* file, which by default is in */etc* unless in your configuration the file is somewhere else, with entries such as..

```
zone "gator.com"  { type master; notify no; file "blackhole.hosts"; };
zone "hotbar.com"  { type master; notify no; file "blackhole.hosts"; };
```

This tells your DNS server to send any queries destined for these domains to the *blackhole.hosts* zone file, and that file has a wildcard entry which will match any query and send it to 127.0.0.1. Try with these two entries for now, restart your DNS server, and try this..

```
 nslookup www.gator.com
```

you should get any answer looking something like this..

```
Name:    www.gator.com
Address:  127.0.0.1
```

Now, there are lots and lots of bad domains out there, here is a list I have, it is already in a format you can use in the DNS server configuration file, just append it to the bottom of the file, but the are some other very good sites on the web that constantly track such things, try the yoyo site or the bleeding edge site. If you use my file you will see there are about 25000-odd domains listed, please feel free to add or remove any you want to.

More Fun
What is not only fun but also useful, is to change the zone file, so that all access point to a website you control that just has a small warning or error page whenever it is accessed. This way everyone trying to access the blackholed sites will see your warning page, but even more useful is that you will have a log of who tried to go where in the access logs of the website. This will make it easy for you to see who is trying to browse bad sites as well as who has a system riddled with spyware.

Final Words

As always with something like this, you use this at your own risk, I am also not saying this is a silver bullet, rather this is another step in a number of steps you will have to take, but it does make a difference and it makes a difference very quickly. Again this paper is limited to a linux box running BIND, but it should not be huge hassle to engineer my list of bad domains into something a different OS or DNS server can use. As always have fun and learn.