FUN WITH NETWORK FRIENDS

by Uriah C.

I enjoy leaving my wireless access point available for others to connect to and use the Internet. There is one catch, however: I get to play and monitor the traffic whenever I want to. In this article, I will describe a pastime that is fun and revealing of your neighbors.

I recently found a new host on my network to play with. New friends are fun! I frequently use EtherApe to quickly monitor my network traffic, and I found a new computer name on my network. Knowing that this person was on my network, I fired up nmap to do a quick ping sweep to confirm my new friend. My new friend's computer name was her real name, and I could see that she had the IP address of 192.168.1.104. The family computer was on 192.168.1.103, my laptop was on 192.168.1.101, and the access point was on 192.168.1.1.

Since I had a new friend to play with, I decided to view the traffic that was going through. Of course I could do that with EtherApe, but I wanted more then just IP addresses and URLs. Besides, I was itching to use the program webspy for a little bit.

Before I go into the fun too much, let me explain what webspy is. Webspy is a program that is part of Doug Song's dsniff suite. These tools are designed to penetration test your network, and, in my case, have fun with those on my network. I must stress that this should only be done on your own network or on one that you have been given permission to preform such tests. Now that the legal stuff is out of the way, let's get on with the fun.

The first thing I have to do is to ARP poison the host and the gateway. This way, the traffic will be routed to my computer. This is done by opening two terminal windows.

In the first terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.1 192.168.1.104
```

In the second terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.104 192.168.1.1
```

Then, I need to make sure that I am forwarding traffic to the proper locations, so I use fragrouter. In a third terminal, type:

```
# fragrouter -i eth1 -B1
```

Now let's see what this does. The first `arpspoof` command sends forged arp information over the interface (`-i`) `eth1` to the target (`-t`) 192.168.1.1 that my computer is 192.168.1.104, while the second terminal tells the target 192.168.1.104 that my computer is 192.168.1.1. Meanwhile, fragrouter sends the broadcast address (`-B1`) all traffic that has come in, so there is no interruption of service.

Now, it's time for the last few steps. I need to run webspy and open a browser. Then, I can have the fun of seeing whatever someone else sees. So, I would open up two more terminals. In the fourth terminal, type:

```
# webspy -i eth1 192.168.1.104
```

And, finally, in the fifth terminal, type:

```
# firefox &
```

Now, Firefox opens up, and I get to see the websites that my new friend opens up in real time. I've only seen one problem: if an ad pops up on a separate page from the rest of a website, it'll be shown separately from the rest of the original site. So, if my friend goes to MySpace, then I see MySpace, but it quickly flashes over to show just the ad without the rest of the site. I have my browser set to open these ads in different tabs, so I can see the page and the ad.

You never know what kind of sites others may visit, so you should do this with discretion—especially if the kids are running around the house and the material coming up is questionable.