

## Re: Wireless LAN got hacked into

---

*Source:* <http://newsgroups.derkeiler.com/Archive/Alt/alt.internet.wireless/2009-05/msg00038.html>

---

- *From:* Yousaf <yousaf.hassan@xxxxxxxxxx>
  - *Date:* Tue, 5 May 2009 05:16:43 -0700 (PDT)
- 

Thanks for replying Jeff. See my comments below:

On May 5, 5:34 am, Jeff Liebermann <je...@xxxxxxxxxxx> wrote:

WEP encryption is an open invitation to hackers. It's now incredibly easy to crack. In my opinion, WEP should be banned from future products.

I have gone back to WPA2 AES once again. The only reason I was checking other encryptions was to enable wireless on my Fedora box. Anyway, it's working now with WPA2 on Fedora with Network Manager.

See the lights on the front of the router and DSL modem. They flash when there's traffic. It takes quite a while to download 4+8GB of whatever. Didn't you notice the lights flashing?

My access point and DSL modem was left on and I am usually out most of the day. I have started to turn it off now. Whenever I get a chance, I monitor active clients using the wireless router admin interface.

<[http://www.edimax.com/en/produce\\_detail.php?pd\\_id=18&pl1\\_id=1&pl2\\_id=5](http://www.edimax.com/en/produce_detail.php?pd_id=18&pl1_id=1&pl2_id=5)>

The Edimax EW-7206APG runs Linux firmware. I think (not sure and too lazy to check) that it supports SNMP out of the box. You can setup MRTG or RRDTool to generate the required traffic history graphs. The catch is that you'll need to leave the Linux box on 24/7 as a data collector. Unfortunately, it appears that the EW-7206APg does NOT support DD-WRT or other alternative Linux based firmware with SNMP.

If not, there's also syslog. I'm again too lazy to check, but if there's a log page, it might allow you some control over what to log. You won't get traffic info, but you will get the URL's and IP's of whatever is generating the traffic.

## Re: Wireless LAN got hacked into

Great! I'll look into this.

Assumption, the mother of all screwups. Any chance you also have a virus infected Windoze box that's been compromised and is spewing spam and garbage all over the internet? If Linux, the most common screwup is to use RDIST or similar synchronization software sending giant files. Ask your ISP is the traffic is mostly incoming or outgoing, which should offer a clue.

Yep. It's more fun to first assign the blame, then confirm the first guess. See "witch hunt" for how it's done.

You definitely have a point here. Another thing I didn't take into account is that my partner started video conferencing (Windows Live Messenger) with her family and friends about two months ago. She had one chat yesterday and the usage stats showed 150MB more! I have to look into this as well.

Yep. That's normally not a common feature. Look into DD-WRT firmware, which does have daily traffic graphs. However, that might require a new wireless access point.

The log files are usually wiped after a power cycle. DD-WRT retains the log files in NVRAM, but that's unusual. More commonly, the traffic data is sent to a syslog server, or collected via an SNMP logger. Some routers also have a feature to email or ftp the syslog file to an email address or ftp server. However, the features are very limited and the content (and passwords) are NOT encrypted. Not recommended.

I won't be able to change my access point but I'll definitely look into other tools you've mentioned.

Is there a router and firewall anywhere in the system, possibly the Linux box? If Linux, it can be used to collect statistics going

Re: Wireless LAN got hacked into

THROUGH the Linux server/router/whatever.

I'll look into this as well.

Thanks again for replying. I'll look into everthing you've mentioned and report back here.

Y

.