

## Re: how to find hidden host within LAN

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2007-11/msg00246.html>

---

- *From:* Chuck <[chuck.carson@xxxxxxxx](mailto:chuck.carson@xxxxxxxx)>
  - *Date:* Sun, 25 Nov 2007 10:27:58 -0800
- 

By the way, I would also recommend placing an IDS (intrusion detection system) in a strategic place in your network. They can be implemented in a manner where they are "hidden" on the network by not using an IP address, these "shadow boxes" as they are called are very usefull in finding stuff like this out. Check out snort and their used to be a decent front end for snort called acid. (not sure if acid is still around or been renamed or whatever – its been years since I worked somewhere they would't spring for a Cisco IDS.

–Chuck

On Nov 25, 2007 6:39 AM, [desant1@xxxxxx](mailto:desant1@xxxxxx) <[desant1@xxxxxx](mailto:desant1@xxxxxx)> wrote:

Hi everybody

I'm using RH ES4 with iptables as gateway/firewall for my LAN.

In the last week i notice in the iptables logs that a host within my lan is doing a lot of traffic.

The destination/source address of the packets and the used port suggest that this host is using peerToPeer application (emule or similar).

The problem is that i'm not able to identify this host within my LAN:

I can see his IP address (192.168.x.

y) and i can find his mac address through ARP, but i can't ping it and there is no host within my lan with this Mac address.

I can't traceroute it.

Can someone help me to find this hidden host?

—

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxx?subject=unsubscribe>  
<http://www.redhat.com/mailman/listinfo/redhat-list>

—

Re: how to find hidden host within LAN

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>