

## trace ip

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2002-07/2303.html>

---

**From:** suse ([suse38@hotmail.com](mailto:suse38@hotmail.com))

**Date:** 07/22/02

From: "suse" <[suse38@hotmail.com](mailto:suse38@hotmail.com)>  
Date: Mon, 22 Jul 2002 05:34:14 -0700

try [www.eamnesia.com](http://www.eamnesia.com) or [www.ripe.net](http://www.ripe.net). eamnesia do a reverse IP search. I found eamnesia gave me more info to track down my hacker!! Good luck.

>-----Original Message-----

> *How can I trace someone trying to hack my ascend digital vpn modem?*

> *posted 07-12-2002 10:04 PM*

> *(post #1)*

>

>

> *I have a small ISP business. Someone has been trying to hack my Lucent*

> *Ascend digital modem box, his last attack I logged he tried 15 or so*

> *different passwords and user names in 1 minute. If he were dialing into it*

> *that number of attempts would be impossible, he has to be already online*

> *with a user account, or accessing it through our router (which is improbable*

> *but not impossible) this unit has RADIUS functions built into it for user*

> *authentication and is being logged into our RAD logs. If he is already*

> *online I assume he could be traced, at least far enough to tell me if he is*

> *one of my users. Am I correct? If so how do I track him and what procedure*

> *should I use to do this?*

>

>

>

>

> *answers:*

>

>you can use arin.net . enter his ip there and it gives  
his ISP. call his ISP  
>and then they will turn him off  
>  
>  
>  
>  
>If he is a smart hacker he will go through one or more  
different networks to  
>hide his true IP address.  
>  
>I may be his ISP...I need to get his IP address to do  
this, unfortunatly  
>this is not one of the things being logged. Thanks for  
your reply though.  
>P.S. He may also be trying to get in through the telnet  
port.  
>  
>Well? I guess you can try setting up some old crappy  
computer you do not use  
>any more and use it as bait?? Put it somewhere on your  
network that will be  
>easy to see from the out side or make the security really  
LAX on that comp.  
>That way I guess you can log him or her from another  
computer so he can't  
>mess around with the computer log files. A bait computer  
is a little easy to  
>spot so install some stuff on that pc that makes it look  
important heh and  
>make sure they, he or her cant use this comp to kill  
other comps on your  
>network... ??? Hope I helped??  
>  
>You Should Get Snort And Portsentry. They Log Attacks and  
The Attackers Ip.  
>This Is Just An Idea.  
><http://www.sourcefire.com/>  
><http://www.psonic.com/products/>  
>  
>  
>I would again suggest snort. [www.snort.org](http://www.snort.org)  
>There is a windows precompiled binary version to  
download . It comes with an  
>extensive help menu so you will be able to figure it out.  
It is all command  
>line so basicly you would go to cmd and then cd\snort  
(presuming installed  
>to c:\) So it will look like this in command  
>  
>C:\Snort>

>Then you would just type out the command you want to run  
in this case u want  
>Intrusion Detection System so the command would be  
>  
>C:\Snort>Snort -dev -l log -h 192.168.1.0/24 -c snort.conf  
>OR  
>C:\Snort>Snort -d -h 192.168.1.0/24 -l log -c snort.conf  
>  
>The snort.conf is the basic configuration files and then  
there are all sorts  
>of other files ranging from DDOS , ICMP , Backdoor ,  
Netbios and a bunch of  
>other stuff. The help file is written for \*nix operating  
systems but with a  
>little bit of patients you will figure out the windows  
commands, Its pretty  
>much just leave out all the ./ out off the command.  
>  
>If you manage to get his IP, NeoTrace for Windoze is a  
wonderful thing. It  
>shows pretty much anything you'll need to know about the  
offending party to  
>shut him down or just have fun with (provided you're that  
kind of sick puppy  
>p-) ! )  
>  
>  
>get his/her ip addy and do the whois to the ip. you can  
try  
><http://www.dwizard.net>  
>  
>  
>  
> quote:  
> (and, from the way you state it, it sounds like  
you're not already  
>logging each and every connection in to that modem box? I  
get that feeling  
>simply from the "last attack I logged" – which implies  
there are some that  
>you didn't... and tÍ{ wÀ | üª ÔÌZ T, ìÆ hat, I'm  
afraid, is a Very Bad Thing (tm))  
>  
>  
>  
>All of the login attempts, (user calls, modem checks  
user/pass with radius  
>database, if ok, then, check Authentication server with  
its radius database,  
>if ok, route user through router to internet ) the router  
should have all

>the proper Cisco filters and blocks in place, we have a certified Cisco  
>networking dood...hehe...CCNA? Anyway I am not too worried about security as  
>my partner in this is certified M\$ and assures me that our system is  
>safe....Although we are working on building a Snort Box for monitoring and  
>tracking. People have tried to crack our safeguards more than once and our  
>system logs show us what they will, only M\$ does not have tracing and  
>tracking services like it should, go figure. We also are going to switch  
>over to a Sun Ultra Sparc 60 we took out of mothballs for use as  
>authentication in the near future. As for our modem box it has never been  
>compromised yet, we change passwords and login names on a scheduled basis,  
>same for our servers.  
>  
>Thanks for all your help and if you guys/girls can think of anything else  
>let me know. I have been a seat-of-the-pants admin since the early '80s and  
>I am self taught in all I know, so if I don't speak the proper jargon please  
>correct me, I am here because I want to learn more, I am a sponge.  
>  
>  
>  
> quote:  
> Originally posted here by aeallison  
> draziw  
>  
> All of the login attempts, (user calls, modem checks user/pass with  
>radius database, if ok, then, check Authentication server with its radius  
>database, if ok, route user through router to internet ) the router should  
>have all the proper Cisco filters and blocks in place, we have a certified  
>Cisco networking dood...hehe...CCNA? Anyway I am not too worried about  
>security as my partner in this is certified M\$ and assures me that our  
>system is safe....Although we are working on building a Snort Box for

>monitoring and tracking. People have tried to crack our safeguards more than  
>once and our system logs show us what they will, only M\$ does not have  
>tracing and tracking services like it should, go figure.  
We also are going  
>to switch over to a Sun Ultra Sparc 60 we took out of mothballs for use as  
>authentication in the near future. As for our modem box it has never been  
>compromised yet, we change passwords and login names on a scheduled basis,  
>same for our servers.  
>  
>  
>  
>  
>Well, I must say that pieces of paper do not "make" an engineer, in my  
>experiences this is especially true when dealing with security (yes I  
>realize that you're not "an Engineer" without those vital pieces of paper,  
>but having them doesn't really mean much anything in the overall picture...  
><edit>eg. doesn't say you know how to troubleshoot worth a darn or do  
>anything specific other than pass some instructor's test to someone's  
>satisfaction</edit> ). The CCNA is, well... it's Cisco's first test and just  
>requires "time" – and I've previously stated my general opinion of the MCSE  
>(particularly of people that have a need to say "oh I'm a MCSE, it's ok" –  
>seems to go hand–in–hand with all these "leet h4ck3r d00ds" if you catch my  
>drift).  
>  
>In my experience, "blindy trus