

## Re: ICMP Killed me and my machine

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-05/3206.html>

---

**From:** Cory Vokey ([cory.vokey@messagingdirect.com](mailto:cory.vokey@messagingdirect.com))

**Date:** 05/31/01

From: "Cory Vokey" <[cory.vokey@messagingdirect.com](mailto:cory.vokey@messagingdirect.com)>  
To: "Mike Silbersack" <[silby@silby.com](mailto:silby@silby.com)>, "Liran Dahan" <[lirandb@netvision.net.il](mailto:lirandb@netvision.net.il)>  
Date: Thu, 31 May 2001 15:27:33 -0600

Using tcpdump, find the source I.P address of who's hitting you and set up a rule using ipfw to block it.

Cory Vokey.

----- Original Message -----

From: "Mike Silbersack" <[silby@silby.com](mailto:silby@silby.com)>  
To: "Liran Dahan" <[lirandb@netvision.net.il](mailto:lirandb@netvision.net.il)>  
Cc: <[freebsd-security@FreeBSD.ORG](mailto:freebsd-security@FreeBSD.ORG)>  
Sent: Thursday, May 31, 2001 3:22 PM  
Subject: Re: ICMP Killed me and my machine

>  
> *On Fri, 1 Jun 2001, Liran Dahan wrote:*  
>  
> > *My machines are being attacked over hours and those are the only*  
*messages i found:*  
> > *Jun 1 00:07:30 freebsd /kernel: Limiting icmp unreachable response from 710*  
*to 20 packets per second*  
> > *Jun 1 00:05:49 freebsd /kernel: Limiting icmp unreachable response from*  
*1092 to 20 packets per second*  
> > *i tonoz of messages like that...*  
> >  
> > *I Had Orange light ON – TRAF on my hub*  
> > *But i was down including all my machines..*  
> >  
> > *–Liran Dahan– ([lirandb@netvision.net.il](mailto:lirandb@netvision.net.il))*  
>  
> *Someone's definitely flooding you. You're going to have to use tcpdump,*  
> *see if you can figure out what's hitting you, and have someone upstream*  
> *filter it. There's probably nothing more you can do on the machines*  
> *themselves.*  
>  
> *Mike "Silby" Silbersack*  
>  
>

FreeBSD–Security: Re: ICMP Killed me and my machine

- > *To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)*
- > *with "unsubscribe freebsd–security" in the body of the message*
- >

To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)  
with "unsubscribe freebsd–security" in the body of the message