

## RE: help: raw\_ip socket and system implication

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2001-12/0000.html>

---

**From:** Mike Price ([mike.price@foundstone.com](mailto:mike.price@foundstone.com))

**Date:** 11/30/01

Message-ID: <5B8559F3126DD4119C5100B0D022A06D0195E869@mailwest.foundstone.com>

From: Mike Price <[mike.price@foundstone.com](mailto:mike.price@foundstone.com)>

To: [vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)

Subject: RE: help: raw\_ip socket and system implication

Date: Fri, 30 Nov 2001 14:34:58 -0800

you can also borrow an unused ip address on the same subnet as the host you are sending from and set this as the source ip for the outbound traffic (use the same mac address as your source host). Then capture packets sent to your host with the destination ip set to the one you are borrowing. your tcp stack will be unaware of this borrowed ip and wont send a RST.

-mike

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

From: Dmitriy Kropivnitskiy [<mailto:dkropivnitskiy@tigertesting.com>]

Sent: Friday, November 30, 2001 11:19 AM

To: [vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)

Subject: Re: help: raw\_ip socket and system implication

I am not sure, I have never tried to do this but looking at the kernel source one notices that in include/linux/socket.h among the options for send() there are a couple called MSG\_RST and MSG\_SYN. They don't seem to appear anywhere else in the kernel source and I couldn't find any docs on them. Otherwise it seems that what you need is somehow register your connection with the kernel.

On Tue, Nov 20, 2001 at 05:36:23PM +0100, [qgiorgi@respublica.fr](mailto:qgiorgi@respublica.fr) wrote:

> hello,

>

> I am trying to figure out a problem i have seen with a

> tcp/ip stack of an equipement, but i need some help in

> order to finish my C code :) I read this mailing-list

> for quite a long time and i am sure there are some

> gurus here :))

>

> I successfully emulate a tcp client for the three

RE: help: raw\_ip socket and system implication

SecurityFocus Vuln-Dev: RE: help: raw\_ip socket and system impl

> *handshake with raw-ip socket (with all the tcp options,*  
> *seq num etc.. i wanted ), but when i received the*  
> *second packet the system send also a RST back to the*  
> *host i am trying to connect to, which is for my system*  
> *point of view an unsolicited SYN/ACK packet.*  
>  
> *so i have*  
> *-> SYN*  
> *<- SYN/ACK*  
> *-> RST ( system part ) :(*  
> *-> ACK ( my prog )*  
> ...  
>  
> *Does anybody have a mean to prevent the system to send*  
> *this RST ?*  
>  
> *Any help will be appreciated :)*  
>  
> *Quentin.*  
>  
> ~~~~~  
> *Découvrez sur Respublica et sur les sites du Groupe Tiscali France*  
> *une barre de navigation pour accéder en 1 clic aux meilleurs contenus*  
> *et services du Web.*  
>  
> *<http://www.libertysurf.fr/minisite/>*  
> ~~~~~  
>  
>

---

• *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)