

Re: IPCOP newbie

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-02/1137.html>

From: Bit Twister (BitTwister@localhost.localdomain)

Date: 02/10/03

From: Bit Twister <BitTwister@localhost.localdomain>

Date: Mon, 10 Feb 2003 01:21:08 GMT

On Sun, 9 Feb 2003 19:10:43 -0600, Darren wrote:

>

> *"Bit Twister" <BitTwister@localhost.localdomain> wrote in message*

> *news:slrnb4duj2.1vv.BitTwister@wb.home...*

>> *On Sun, 9 Feb 2003 18:56:33 -0600, Darren wrote:*

>> > *Can somebody explain to me the difference in the firewall log files of*
> *the*

>> > *source port and destination port. Is it safe to say the destination*
> *port*

>> > *is the port it is trying to penetrate, but I do not understand why there*
> *is*

>> > *various source ports?*

>>

>> *If I was to scann your pc, the source port would be the port I use*

>> *to scan your pc with. The destination port is the port I chose*

>> *to try on your boex. My source port would depend on my hardware/software*

> *setup.*

>>

>>

>> > *Sorry for the newbie question.*

>> > *Also what is the difference between the intrusion detection system logs*
> *and*

>> > *the firewall logs??*

>>

>> *Depending on how your set them up, the firewall logs all hits on your*

>> *box. IDS could log hits which it thinks are intrusion attempts.*

>

> *Thanks for you reply, the first answer makes sense to me, but the second*
> *question,*

> *just curious, isn't all logged items an intrusion attempt?*

That is one of the problems. You turn on logging for all hits on your firewall and you will soon quit looking at all that noise.

The IDS could detect someone hitting your box once a week.

The firewall might pass a connection through where an IDS might notify you of a malformed packet.