

Re: I

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-03/0088.html>

From: Adie (a_usenetizen@hotmail.com)

Date: 03/01/03

From: Adie <a_usenetizen@hotmail.com>

Date: Sat, 01 Mar 2003 17:42:54 +0000

[bob, usenet posts aren't supposed to be anonymous – please leave attributes in for whom you're replying to. It's also considered appropriate to place [snip] where have edited the original article.]

bob wrote:

>Adie wrote:

>> *Sure but on a network you have remote access, and machines logging
>> information delivered by and produced by other machines. For instance
>> it's more than feasible to build a packet with spoofed headers which
>> will be logged as normal, in which case how do you track who put the
>
>Sometimes that's the case.*

Well fer crying out loud, you've nothing left to argue about – I win.

>*There are also cases where, for instance, I
>can pull the wire out of the network closet that goes to one particular
>machine and plug it in the back of a firewall box. Now with \$200 worth of
>hardware I have isolated the suspect computer from the universe. The NIC
>on the suspect box is wired straight to the NIC on my box. There is no
>doubt where the packets originate.*

Fine. I'm sure there are numerous methods of isolating, all of which take the kind of proactive stance which is rare in a small business – many large organisations too.

>> *Furthermore, the costs to the business of going to court to fire
>> someone over looking at a pair of tits will no doubt be prohibitive,
>
>You notice that in the cases cited, the network was used in such a way as
>to catch the guilty party in the act.*

So someone has to be sitting around waiting for the user to offend. Like I said – very few can afford to take such measures.

comp.security.firewalls: Re: I

>> *All those "expert witnesses" don't come cheap.*

>

>*They aren't necessary when the rent-a-cops catch the guilty party doing
>his thing. There's not much point in the guilty even taking that one to
>trial.*

Bit of an extreme example wasn't it? I suspect the offence is "lewd
conduct in a public place" or some such, illegal with or without a
computer.