

FreeBSD–Security: Re: (no subject)

Re: (no subject)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-01/0556.html>

From: FBSDSecure@aol.com

Date: 01/30/01

From: FBSDSecure@aol.com

Date: Tue, 30 Jan 2001 03:00:42 EST

To: freebsd-security@freebsd.org

In a message dated 1/28/01 12:43:34 PM Pacific Standard Time, root@noops.org writes:

> > *On Sun, 28 Jan 2001, Chris wrote:*

> > > *Another thing to point out though is if a hacker were to spoof his IP*

> *address*

> > > *and do a port scan, what would be the point? The data is useless if it can't*

> > > *get back to the individual.*

> > >

> > > *One word, DoS.*

>

> *Well, two words... one of which is DoS. Another, which I find fun, and also doesn't matter if your ISP does egress filtering is to make a scan look like it came from your whole subnet. I'm sure that even if my DSL provider was making sure all the leaving traffic came from it's network it would still be tough to catch. Or, and this is rare these days, is if you are on an unswitched subnet or could somehow view traffic in flight you can always make the scan look like it came from the guy next door and just sniff the replies as them come back.*

>

> *I know my DSL is unfiltered on it's way out, so if I'm doing an audit from home for any reason I always mix in 127.0.0.1 as a decoy -- just in case it hits something amusingly misconfigured, like a portsenry-type package with a glaring misconfiguration.*

>

> *-tcannon*

>

That's why 127.0.0.1 is in the ignore file. Reminds me of an phrase I heard somewhere...One false packet and I'll knock you off the net....Or something like that.

Dan.

Re: (no subject)

FreeBSD-Security: Re: (no subject)

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message