

Re: Misconceptions

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-01/1508.html>

From: JR (notlikely@nowhere.com)

Date: 01/14/03

From: "JR" <notlikely@nowhere.com>
Date: Mon, 13 Jan 2003 19:15:40 -0500

"Leythos" <void@nowhere.com> wrote in message
news:MPG.188d130e6a20117798993e@news-server.columbus.rr.com...
> In article <[LnAU9.46186\\$L47.6959148@read2.cgocable.net](mailto:LnAU9.46186$L47.6959148@read2.cgocable.net)>,
> notlikely@nowhere.com says...
>> *What some contributors to this newsgroup seem to need, is a better
>> understanding of the devices and technologies commonly referred to here.*
>>
>>
>>
>> *There seems to be some confusion on what does what. In
>> comp.security.firewalls FERRANTE (Mark) recently asked "Is a router a
good
>> firewall?" That is akin to asking "is a bus is a good airplane". Just
>> because a bus can fly off a cliff or perform a stunt as in the movie
>> "Speed", does not qualify it as an airplane!*
>>
>>
>>
>> *True routers route traffic much like the old railroad turntables
>> (<http://www.railroadextra.com/roundtab.html>) were used to redirect
>> locomotives when there was more than one path they could take. If there
are
>> only two pieces of track leading to the turntable, then the routing
function
>> is void and simply becomes a relaying function.*
>>
>> *Routers can implement "access control lists", a rudimentary form of
>> filtering, but that does not make them a "firewall".*
>>
>>
>>
>> *NAT can be implemented on many routers, but only on stub network (the
last
>> leg of a route, usually a private/office network) routers. The original
>> intent for NAT (see RFC1631) was a stop gap measure to overcome the
>> increasing shortage of legitimate IPs (RFC1918). The fact that internal*

comp.security.firewalls: Re: Misconceptions

> > *private address ranges were masked from public view was a side benefit as a*
> > *result of the translation, not an intentional security measure.*
> >
> >
> >
> > *Routers are NOT firewalls. Firewalls implement security policies or rules*
> > *and work closely with routers or routing functions. Firewalls either allow*
> > *or deny packets based on the implemented rules. Any good firewall uses SPI*
> > *(Stateful Packet Inspection) and PAT (Port Address Translation) as opposed*
> > *to its lesser cousin NAT.*
> >
> > *Routers do not use SPI and PAT. If they do, then they are Router/Firewalls.*
> >
> >
> >
> > *Routers and Firewalls do not perform any anti-virus functions. These are*
> > *handled by (surprise, surprise) anti-virus programs, which should be on the*
> > *individual client machines if the firewall/router/NAT functions are on a*
> > *separate, dedicated machine (as opposed to a network consisting of one*
> > *computer). Anti-virus programs use pre-defined virus signatures and*
> > *heuristic methods (on the better ones).*
> >
> >
> >
> > *A NIDS (Network Intrusion Detection System) is just that. It can be a*
> > *combination of programs that alerts the system of attempted intrusion.*
For
> > *example, receiving a stream of FIN packets is not normal, and is therefore*
> > *reported by the NIDS as a possible port scan, normally the prelude to an*
> > *attack. Although Black Ice NIDS apparently has heuristic capabilities, that*
> > *would be an anti-viral component working in conjunction with the NIDS, but I*
> > *am not experienced with Black Ice.*
> >
> >
> >
> > *This rant is not meant to insult or offend anyone, but it would be nice to*
> > *keep facts and information somewhat correct.*
> >
> >
> >

comp.security.firewalls: Re: Misconceptions

> > *If anyone finds the above info incorrect, let me know, and back it up
with
> > VALID documentation.*
>
> *I liked this post so much that I won't even snip it when I reply!*
>
> *This post has hit the proverbial nail 100% on the head – and I keep
> trying to say this same thing to people that insist that a router/nat
> box is a firewall (it's not).*
>
> *I think that you summarized everything perfectly! Congratulations – keep
> up the good work.*
>
>
> --
> --
> Leythos999@columbus.rr.com
> *(Remove 999 to reply to me)*

thank you....appreciate the comment
JR