

Re: Network scanning

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-08/0305.html>

From: White-Tiger (white-tiger_at_rocketmail.com)

Date: 08/09/03

Date: Sat, 9 Aug 2003 08:18:58 -0700 (PDT)

To: Sebastian Schneider <ses@straightliners.de>, CHRIS GRABENSTEIN <LFGRABC@LF.VCCS.EDU>, security

I am sorry I got on this late... Some switches support eapol that works with a radius server to auth mac address at port level before the switch will enable that port... I have done limited testing. If you unplug a live connect, not only will someone be calling saying that something doesn't work, but when they plug in there NIC the switch will see a new MAC and disable the port.

Some one can give some ideas about MAC spoofing, But doesn't the NIC give its real MAC to the switch while you are trying to spoof someone elses MAC?

if this is the case, then you can disable and port that is not a known MAC.

I have a baystack450, and I can setup the MAC in each of the switches, but that will be kinda hard to maintain. So I am looking at free radius for OpenBSD that supports eapol, so I can just setup a file with all allowed MACs.

Hope this helps, sorry if someone already said this, I am a little late on the thread.

WT

--- Sebastian Schneider <ses@straightliners.de> wrote:

> On Friday 08 August 2003 14:19, CHRIS GRABENSTEIN wrote:

>

> > As far as the hard wires, I think the best solution is
> to search out those

> > unused ports and unplug them from the switch. They can
> be quickly

> > reconnected if needed, and you'll know about it.

>

> I guess you're actually aware, that not everyone is
> locking up rooms

> containing switches.

SecurityFocus BASICS: Re: Network scanning

> *And just plugging out unused cables won't be sufficient,*
> *since usually*
> *I just can plug out any computer and plug in my own.*
>
>
>> |-----Original Message-----
>> |From: netsec novice [mailto:netsec9@hotmail.com]
>> |Sent: Thursday, August 07, 2003 4:51 PM
>> |To: security-basics@securityfocus.com
>> |Subject: Network scanning
>> |
>> |
>> |Are there tools out there that would allow system
> administrators to be
>> |notified when a new workstation attaches to a network?
> I'm
>> |thinking both
>> |wireless and ethernet in this case. SNMP maybe? I am
> in a
>> |credit union
>> |environment and my concern is that someone would be
> able to steal an
>> |existing jack or a jack that is not physically
> protected but
>> |live and be
>> |able to capture traffic or do reconaissance. We don't
> have
>> |Wireless access
>> |at this point but may look to it in the future. My
> only
>> |thought in that
>> |case would be to encrypt all traffic since wireless
> security
>> |is a bit scary
>> |at this point. Any ideas?
>>
>>
>

>>
>

>> -
>
> --
>
> -----
> straightLiners IT Consulting & Services
> Sebastian Schneider
> Metzger Str. 12
> 13595 Berlin

SecurityFocus BASICS: Re: Network scanning

- > *Germany*
- >
- > *Phone: +49-30-3510-6168*
- > *Fax: +49-30-3510-6169*
- > *Mail: ses@straightliners.de*
- >
- >
- > *Diese E-Mail enthält vertrauliche und/oder rechtlich*
- > *geschützte Informationen.*
- > *Wenn Sie nicht der richtige Adressat sind oder diese*
- > *E-Mail irrtümlich*
- > *erhalten haben,*
- > *informieren Sie bitte sofort den Absender und vernichten*
- > *Sie diese Mail.*
- > *Das unerlaubte Kopieren sowie die unbefugte Weitergabe*
- > *dieser Mail ist nicht*
- > *gestattet.*
- >
- > *This e-mail may contain confidential and/or privileged*
- > *information.*
- > *If you are not the intended recipient (or have received*
- > *this e-mail in error)*
- > *please notify the sender immediately and destroy this*
- > *e-mail. Any unauthorized*
- > *copying,*
- > *disclosure or distribution of the material in this e-mail*
- > *is strictly*
- > *forbidden.*
- >
- >

>

>

Do you Yahoo!?
Yahoo! SiteBuilder – Free, easy-to-use web site design software
<http://sitebuilder.yahoo.com>
