

RE: Securing a Local Network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-04/0257.html>

From: Meidinger Chris (chris.meidinger_at_badenit.de)

Date: 04/19/04

To: webmaster <webmaster@play-by-mail.de>, roberts@tridecap.com, security-basics@securityfocus.com
Date: Mon, 19 Apr 2004 20:14:34 +0200

On re-reading, I would like to clarify what I mean by 'allow a lot of different ports on the local network.' I mean that, particularly if these are windows hosts, you will probably have to open at least 135,-7,-9 to source IP's from your local net. That will make it relatively easy for an attacker that has broken into one host to hop among the other hosts.

If you have a central firewall acting as a choke point, you can at least limit the possibilities an attacker has. You can make it impossible for computers to go out over non-essential ports, as well as prevent internet hosts from opening any connections inside.

When you said that your machines are behind NAT, I was thinking 'classic' NAT in that each machine has an Internet IP assigned to it on the other side of the NATting device. If you mean that your router is doing masquerading or port overloading, so that each outbound connection is statefully tracked, then the considerations I brought up are less meaningful. I assume, however, from your post that you are not.

Cheers,

Chris Meidinger

> -----Original Message-----
> From: Meidinger Chris [<mailto:chris.meidinger@badenit.de>]
> Sent: Monday, April 19, 2004 8:27 AM
> To: webmaster; roberts@tridecap.com; security-basics@securityfocus.com
> Subject: RE: Securing a Local Network
>
> Hallo Andreas,
>
> there are definitely advantages to using a proper firewall,
> beyond simple defense in depth. The primary one, is that you
> will have to allow a lot of different ports on the local
> network. That means that the compromise of a single
> misconfigured host will result in the compromise of the
> entire network. What about, for example, a virus or trojan? A
> desktop firewall will not likely protect from call-home

SecurityFocus BASICS: RE: Securing a Local Network

> *malware that opens a connection itself to an internet host*
> *waiting for a shell. For this and other reasons, conventional*
> *wisdom dictates that a central chokepoint be created, where*
> *you can make a strong divide between the internal and*
> *external network.*
>
> *If you use a dedicated firewall, there is absolutely no*
> *reason not to use desktop firewalls. Simple defense in depth*
> *is an advantage, but if you can correlate logs, desktop*
> *firewalls can also turn into a sort of IDS to alert you if an*
> *internal host is scanning or exploiting machines.*
>
> *If you want to talk at more length or in german, feel free to mail,*
>
> *Cheers,*
>
> *Chris*
>
> > -----Original Message-----
> > *From: webmaster [mailto:webmaster@play-by-mail.de]*
> > *Sent: Thursday, April 15, 2004 11:21 AM*
> > *To: roberts@tridecap.com; security-basics@securityfocus.com*
> > *Subject: Re: Securing a Local Network*
> >
> > *Hi John,*
> >
> > *even if you have a virus protection at the gateway, you*
> > *still need it*
> > *on the clients. People use usb-sticks, notebooks and things*
> > *like that.*
> > *Another problem is the fact, that gateway protection cant*
> > *protect you*
> > *against password protected email attachments. So the best way is a*
> > *combination of both. If you want to save money, give up*
> > *fileserv-er-protection.*
> >
> > *I have got 2 other questions, regarding your issue, which might be*
> > *interesting for you, too.*
> >
> > *If I do not host my own services, is there a advantage to*
> > *protect my*
> > *network through a packetfilter or even a statefull*
> > *inspection firewall*
> > *appliance? Or is it enough to use NAT in combination with personal*
> > *firewalls on every desktop?*
> >
> > *If I use a firewall appliance, do I still need personal*
> > *firewalls on*
> > *the desktops? I guess I do. One benefit are internal attacks using*
> > *tools like superscan. Am I right?*
> > *Other benefits?*

SecurityFocus BASICS: RE: Securing a Local Network

>>
>> *Regards*
>> *Andreas*
>>
>> *John Roberts wrote:*
>>
>>> *I started working as a sys admin at a small company (about*
>> *15 people)*
>>> *and they are starting to think it's time to upgrade their*
> *network.*
>>> *Right now it's just 20 computers, running a mix of xp and*
> *2000 on a*
>>> *local network, sharing files, with almost no anti virus and*
>> *the only*
>>> *protection from the outside world is the NAT that the*
>> *routers perform.*
>>>
>>> *I've tried to get the to upgrade to a domain, add a file*
> *server for*
>>> *backup, get some office wide virus protection and maybe*
>> *even take our*
>>> *email in house, but they've balked at the price to setup a legit*
>>> *windows domain. The main goals are access control on the local*
>>> *network and virus / worm protection. I'm suggesting a*
>> *Windows domain*
>>> *controller to enforce access control and then an centralized*
>>> *anti-virus product. Is this enough, and are there other (easier,*
>>> *cheaper, more effective ways) to make sure that only the*
> *people who*
>>> *need to can access the financial records, the computer people can*
>>> *access the all computers when they need to, and some user*
>> *decides to download a cute little program won't destroy the whole*
> *network with a virus.*
>>>
>>> *Is a linux domain controller a solution, considering*
>> *everything else*
>>> *in house is windows? Is an anti-virus solution at the*
>> *gateway better*
>>> *than an anti-virus solution on each desktop? Basically,*
>> *what's a good*
>>> *way to set up a solid base of network security, which can*
>> *then be expanded on?*
>>>
>>> *John Roberts*
>>>
>>>
>>
>

>>> ----- *Ethical Hacking at the InfoSec Institute. Mention*
> *this ad and*

SecurityFocus BASICS: RE: Securing a Local Network

> > > *get \$545 off any course! All of our class sizes are*
> > *guaranteed to be*
> > > *10 students or less to facilitate one-on-one interaction*
> > *with one of*
> > > *our expert instructors.*
> > > *Attend a course taught by an expert instructor with years of*
> > > *in-the-field pen testing experience in our state of the*
> *art hacking*
> > > *lab. Master the skills of an Ethical Hacker to better*
> > *assess the security of your organization.*
> > > *Visit us at:*
> > >
> >
> >
> http://www.infosecinstitute.com/courses/ethical_hacking_training.html
> > >
> >
>

> > > -----
> >
> >
> > -----
> > -----
> > *Ethical Hacking at the InfoSec Institute. Mention this ad*
> *and get \$545*
> > *off any course! All of our class sizes are guaranteed to be 10*
> > *students or less to facilitate one-on-one interaction with*
> *one of our*
> > *expert instructors.*
> > *Attend a course taught by an expert instructor with years of*
> > *in-the-field pen testing experience in our state of the art hacking*
> > *lab. Master the skills of an Ethical Hacker to better assess the*
> > *security of your organization.*
> > *Visit us at:*
> >
> http://www.infosecinstitute.com/courses/ethical_hacking_training.html

> > -----
> >
> >
> > -----
> > -----
> > *Ethical Hacking at the InfoSec Institute. Mention this ad and*
> *get \$545 off any course! All of our class sizes are*
> *guaranteed to be 10 students or less to facilitate one-on-one*
> *interaction with one of our expert instructors.*
> *Attend a course taught by an expert instructor with years of*
> *in-the-field pen testing experience in our state of the art*
> *hacking lab. Master the skills of an Ethical Hacker to better*
> *assess the security of your organization.*
> *Visit us at:*

SecurityFocus BASICS: RE: Securing a Local Network

> http://www.infosecinstitute.com/courses/ethical_hacking_training.html

> -----

> -----

>

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors.

Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
