

RE: A question about a basic security setup...

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-12/0197.html>

From: Keith.Morgan (Keith.Morgan@Terradon.com)

Date: 12/05/01

From: "Keith.Morgan" <Keith.Morgan@Terradon.com>

To: "'security-basics@securityfocus.com'" <security-basics@securityfocus.com>

Date: Wed, 5 Dec 2001 14:11:04 -0500

Comments in line.

> -----Original Message-----

> **From:** Bill Walls [<mailto:stauph@hotmail.com>]

> **Sent:** Monday, December 03, 2001 3:41 PM

> **To:** security-basics@securityfocus.com

> **Subject:** A question about a basic security setup...

>

>

> I have been thinking about a setup for my basic ADSL network

> at home that

> would be somewhat more secure then the usual setup I have

> seen around for

> other users who simply think NAT/Firewalls are the answer. I

> have yet to

> impliment it, but I wonder if someone could critique the

> abstract idea

> before I go through motions of setting up the network.

NAT and firewalls help. Not a complete solution, but they help.

>

> The reason why I go into so much details is that I am testing my own

> knowledge against yours to become a better security minded

> user. I don't

> want my box trying to break into your box. ;)

>

> I have a cisco 678 router (Which I have disabled the telnet

> as well as web

> interface and set the ports to different ports then the

> default.) Since it

> it only interfactable through the management cable, I don't

> fear a breach for

> the router software itself. I do know that if someone where

> to find the

> telnet port, a DoS is possible. And it is using NAT.

SecurityFocus BASICS: RE: A question about a basic security setup...

It looks like you plan on doing what you can here. Good so far.

>
> *I am running a web server (apache) on port 80. The nat*
> *addresses this*
> *machine for all port 80 requests. Every machine on the*
> *network is running a*
> *form of firewall software, on windows zone alarm, on linux*
> *either ipchains*
> *or iptables.*

I don't know if this is relevant, but were it an IIS box, I would configure it with appropriate host-header names (virtual servers in apache).

In IIS this causes remote hosts that request pages and (and exploitable dll's and such) to receive the "no site configured at this address" response. With apache, a minor issue, but maybe a detail worth looking into.

>
> *I am thinking of putting a dual-homed host to make the basic*
> *network look*
> *like thus:*
>
>
> +-----+
> | Cisco 678|
> +-----+
> |
> +-----+
> |Dual-Home Host|
> +=====+
> |
> +-----+
> |USR Totalswitch|
> +=====+
> |
> *Other boxes including web server.*
>
> *I know the USR Totalswitch is completely insecure. On my*
> *firmware, I cannot*
> *turn off the telnet management port and I cannot protect*
> *against the debug*
> *attack found in the securityfocus archives. Is there a*
> *firmware version that*
> *allows for more security? I have yet to find it. Anyway...*

If they get as far as being able to connect to the switch, you've lost the battle.

SecurityFocus BASICS: RE: A question about a basic security setup...

- >
- > *I was thinking of running iptables on the dual homed host,*
- > *and snort. I am*
- > *researching snort heavily at the moment to make sure I*
- > *understand it's*
- > *capabilities. I am more of an ipchains kinda guy, and have*
- > *just delved into*
- > *iptables.*

Snort is fantastic. And, allow me to say this, if you thought ipchains was good, you will be **very** impressed with iptables. The addition of stateful inspection to the 2.4 kernels has added an immense amount of power and control to an already good packet-filtering solution. IMHO, iptables provides you 100% of the raw firewalling capability normally found in expensive commercial firewalls.

- >
- > *What I want to do is make it so only legit GET requests get*
- > *to my web server*
- > *machine. I.e. GET / HTTP/1.x etc etc and to drop all other kinda of*
- > *requests. My feeling on the subject is if I can filter out all other*
- > *malformed requests or unrealistic requests, apache will be*
- > *"saved" from the*
- > *majority of attacks.*

Hmmm, you're going outside the abilities of either iptables or snort at this point. Snort passively monitors the wire generating alerts when aforementioned "bad" stuff happens. Iptables provides you stateful firewalling.

What you are looking for here, is an "application proxy" type firewall. These work above layer 3 and are aware of such things as GET, POST, etc. I'm not aware of a freeware/GNU solution in an application proxy firewall. If you find one, **please** let me know.

- >
- > *Should I use snort or iptables to accomplish this? Is it*
- > *possible with*
- > *either? I know I should RTFM...and believe me, I am. But I*
- > *was wondering*
- > *what kind of input I could get from the list as a whole as*
- > *how to proceed.*
- > *I have also been toying with the idea of using LIDS on the*
- > *server machine to*
- > *throw even more modification into the mix...*
- >
- > *I guess this is just a call for comments. Thank you for*

RE: A question about a basic security setup...

SecurityFocus BASICS: RE: A question about a basic security setup...

- > *considering this*
- > *issue...as it will determine some of my future turns in study*
- > *for security*
- > *as a whole.*

As a whole, your planned setup looks pretty solid to me. Spend some resources in hardening apache and hardening the iptables/snort machine, and you should be golden. While i'm one of those annoying people that insists that *nothing* is 100% hacker-proof, the setup you describe here will make you an unattractive target. The cost in time and money involved in breaching your proposed setup is likely considerably higher than the value of the information you wish to protect in your home LAN. That's the whole point of information security. Make it un-attractive, make it difficult.

- >
- > *"Buffer Overflow in /dev/stomach due to vodka.o!"*
- >
- >
- >
- > _____
- > *Get your FREE download of MSN Explorer at*
- > *<http://explorer.msn.com/intl.asp>*
- >

-
- ***Previous message:*** Jason Kohles: "Re: pix firewall and mail server"
 - ***Maybe in reply to:*** Bill Walls: "A question about a basic security setup..."
 - ***Next in thread:*** Aaron Peterson: "Re: A question about a basic security setup..."
 - ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]