

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

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-12/0245.html>

From: dewt (dewt@kc.rr.com)

Date: 12/06/01

From: dewt <dewt@kc.rr.com>

To: "Bill Walls" <stauph@hotmail.com>, security-basics@securityfocus.com

Date: Thu, 6 Dec 2001 08:35:27 -0600

On Monday 03 December 2001 02:40 pm, Bill Walls wrote:

> 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.

>

> 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 interfacable 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.

>

> 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.

>

that setup is far in excess of most home users and most corporate setups,
however finding the www administration port on your router would be a trivial
task. you might want to consider blocking it on the external interface.

>

> I know the USR Totalswitch is completely insecure. On my firware, 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 verison
> that allows for more security? I have yet to find it. Anyway...

>

with your front end so secure, and each of your client machines locked down,
a compromised switch is very highly unlikely. try and find the firmware
upgrade if it exists, but it's not worth losing sleep over if the rest of the
network is rock solid.

> I was thinking of running iptables on the dual homed host, and snort. I am

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

- > 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.
- >
- > 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.
- > 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 think you could do that with hogwash it's available at

hogwash.sourceforge.net , you'd have to make a custom rule of course

- > I guess this is just a call for comments. Thank you for considering this
- > issue...as it will determine some of my future turns in study for security
- > as a whole.

>

> "Buffer Overflow in /dev/stomach due to vodka.o!"

>

>

lemme just say that if more people had security layouts like this one we'd see a lot fewer worms, ddoses, and whatever. it's nice to see that there are some people as paranoid as me when it comes to even home machines

-
- **Previous message:** [Tim Blangger: "Stealther"](#)
 - **In reply to:** [Bill Walls: "A question about a basic security setup..."](#)
 - **Next in thread:** [Hornat, Charles: "RE: A question about a basic security setup..."](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)