

[fw-wiz] UNSUBSCRIBE

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-05/0099.html>

From: Delong, Jeff E. (*DelongJE_at_westinghouse.com*)

Date: 05/20/05

To: "'firewall-wizards@honor.icsalabs.com'" <firewall-wizards@honor.icsalabs.com>

Date: Fri, 20 May 2005 08:23:20 -0400

-----Original Message-----

From: firewall-wizards-request@honor.icsalabs.com

[mailto:firewall-wizards-request@honor.icsalabs.com]

Sent: Thursday, May 19, 2005 7:14 PM

To: firewall-wizards@honor.icsalabs.com

Subject: firewall-wizards digest, Vol 1 #1585 - 8 msgs

Send firewall-wizards mailing list submissions to
firewall-wizards@honor.icsalabs.com

To subscribe or unsubscribe via the World Wide Web, visit
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
or, via email, send a message with subject or body 'help' to
firewall-wizards-request@honor.icsalabs.com

You can reach the person managing the list at
firewall-wizards-admin@honor.icsalabs.com

When replying, please edit your Subject line so it is more specific than
"Re: Contents of firewall-wizards digest..."

Today's Topics:

1. Re: Extreme Problem with PIX Config (Devdas Bhagat)
2. Re: A fun smackdown... (Paul D. Robertson)
3. Re: A fun smackdown... (Paul D. Robertson)
4. Re: A fun smackdown... (Chuck Swiger)
5. Re: A fun smackdown... (Paul D. Robertson)
6. Re: A fun smackdown... (Devdas Bhagat)
7. Re: A fun smackdown... (Chuck Swiger)
8. Re: A fun smackdown... (Paul D. Robertson)

--_--_--_--

Message: 1

Date: Fri, 20 May 2005 02:58:34 +0530

Firewall-Wizards: [fw-wiz] UNSUBSCRIBE

From: Devdas Bhagat <devdas@dvb.homelinux.org>
To: firewall-wizards@honor.icsalabs.com
Subject: Re: [fw-wiz] Extreme Problem with PIX Config
Reply-To: Devdas Bhagat <devdas@dvb.homelinux.org>

On 10/05/05 09:14 -0500, Brian Loe wrote:

<snip>

> *domain-name domain.com*

If you are munging, please use example.com/example.net/domain.invalid

> *fixup protocol dns maximum-length 512*

This breaks EDNS. You will have issues with this if you run a system behind the pix checking DNSBLs. Run a decent caching DNS server internally as a proxy.

> *fixup protocol ftp 21*

Why allow this in the first place?

> *fixup protocol h323 h225 1720*

> *fixup protocol h323 ras 1718-1719*

> *fixup protocol http 80*

> *fixup protocol icmp error*

> *fixup protocol rsh 514*

Again, why proxy something which you should not be allowing at all?

> *fixup protocol rtsp 554*

> *fixup protocol sip 5060*

> *fixup protocol sip udp 5060*

> *fixup protocol skinny 2000*

> *fixup protocol smtp 25*

Unless you are defending MS Exchange, turn this off. This breaks ESMTP, including the useful SMTP AUTH and TLS extensions. Actually, turn this off anyway and put in Postfix or Exim behind this box to act as a ESMTP proxy.

> *fixup protocol sqlnet 1521*

> *fixup protocol tftp 69*

Repeat proxy question.

Devdas Bhagat

-- __-- __--

Message: 2

Date: Thu, 19 May 2005 17:32:21 -0400 (EDT)

From: "Paul D. Robertson" <paul@compuwar.net>

To: Chuck Swiger <chuck@codefab.com>

Cc: firewall-wizards@honor.icsalabs.com, Martin <marty@supine.com>

Subject: Re: [fw-wiz] A fun smackdown...

[fw-wiz] UNSUBSCRIBE

On Thu, 19 May 2005, Chuck Swiger wrote:

> >>> *_All_ effective security controls break that tenet. The more*
> >>> *liberal your controls, the more risk you assume.*
> >>
> >> *There is more to an effective security control than only denying*
> >> *stuff!*
> >
> > *No, there isn't in terms of the mitigation of risk. Anything else*
> > *isn't about the security properties of the control, but about its*
> > *operational effectiveness. _What_ you deny, _how_ well it's*
> > *implemented, and where you deny it is in fact the essence of*
> > *security. From guards with guns to*
> > *firewalls to anti-virus, default deny or default except- either one*
> > *works*
> > ^^^^^
> > *by blocking stuff (what you know is bad, or what you don't know is*
> > *acceptable.)*
>
> *"default accept", you mean? Sure, there are two general approaches:*

Yep brain fumble...

> *"deny all, and then have a list of stuff to permit", or "permit all,*
> *and then try to deny stuff known to be bad".*

But both of them rely on blocking things, either known-bad, or unknown.

> *The former approach is a lot more likely to result in a secure system,*
> *but both approaches do more than just deny everything: what you*
> *accept, how well it's implemented, and where you accept stuff [to*
> *paraphrase] is also the essence of security.*

I never said they denied everything- I said they worked by blocking stuff.
In terms of security, what you accept is what you haven't blocked. If
you're not blocking, then you're not adding security controls.

> *Choosing to provide remote shell access via SSH is better than using*
> *Telnet or a VPN. Choosing to provide POP or IMAP via SSL is better*
> *than choosing to provide remote mail access via plaintext with*
> *passwords passed in the clear. If you can live without either, by all*
> *means, forbid remote access.*

That's the point, the more you accept, the more risk you accept. The more
you block, the less risk.

> >> *I think you're over-valuing the utility of "deep protocol*
> >> *inspection",*
> >
> > *Um, what the heck does "deep protocol inspection" have to do with*
> > *the fact that security controls are a denial technology? Where*

> > *exactly did I say*
> > *anything about deep protocol inspection?*
>
> *You are disagreeing with a design principle from the RFC's which*
> *discusses how to create robust software protocols. One could provide*
> *other examples.*

No, I'm not disagreeing with it, I'm saying that it's not relevant to security because security controls are automatically less than liberal. Creating robust protocols isn't the same thing as providing security, would that more protocol designers understood that.

> > > *Paul, and you seem to be ignoring the risks of denying legitimate*
> > > *connections which should have been permitted.*
> >
> > *No, again— Security works by denying things. That's got nothing to*
> > *do with falsely denying things, and everything to do with accepting*
> > *risk. If I deny everything, my risk is lower than if I deny 90% of*
> > *everything— but*
> > *in either case, the security factor is about denying.*
>
> *Paul, why *don't* people run their firewalls with a single "deny all"*
> *rule?*

Again, that's got **nothing** to do with the fact that firewalls work by denying traffic. It also has nothing to do with the fact that accepting less stuff == less risk. The part where the rubber meets the road is in deciding which risks to allow and which stuff is necessary. That doesn't mean more stuff won't increase your risk, and it doesn't mean that security controls don't work by blocking stuff, both of which were my original points.

> > > *An effective security measure needs to implement the security*
> > > *policy. It needs to permit the types of access that legitimate*
> > > *users are allowed to have, for the system— meaning the network,*
> > > *the firewall, and the server(s) or other equipment being used— to*
> > > *work correctly.*
> >
> > *That doesn't change the fact that it all works by denying things,*
> > *not by liberally accepting just anything that might come over the*
> > *wire.*
>
> *I didn't say, "accept anything", I said, accept the types of access*
> *that the security policy says are permitted.*

Which means denying everything else. Again, you're trying to put words into my mouth. Security polices don't have anything to do with my original points.

> > > *This is just as important as denying access to stuff that is not*
> > > *permitted by the security policy.*

> >
> > *That's not a security property though, it's an operational property.*
> > *Now, you can argue that denying too much impacts business, and I'd*
> > *agree, because it doesn't conflict with what I said–*
> >
> > *1. Security things work by blocking stuff.*
> > *2. The less stuff you block, the more risk you assume.*
>
> *If my key doesn't open my front door, it's blocking legitimate access.*
> *A security system which prevents legitimate access is a broken*
> *security system.*

No, that's a risk/reward choice that's made by the security policy. It's perfectly acceptable to have false positives in some situations. It may in fact, be designed in because the cost of loss is so great that having some denied legitimate access is worth reducing the overall risk. Just because it's not **convenient** doesn't mean it's broken. Rate of false positive is, just like rate of false negative something that's part of the "should I do this?" equation, not the "is this secure" equation.

It may be that you're roaring drunk, and if you got in, you'd throw things around, or accidentally drop a lit candle on the floor and burn the place down– so there is still less risk if you key doesn't work, it's just then not as useful for you as a door (or like most users, you'll just leave it unlocked.)

> > > *Has "fixup protocol smtp 25" actually done much to prevent a*
> > > *vulnerable M\$ Exchange box from being owned, or helped control the*
> > > *flow of spammy/virusized traffic significantly? Does it help*
> > > *control outbound*
> >
> > *I don't know what it does, since I don't field PIXes and have only*
> > *worked on two in my entire life; but I _assume_ that it will block*
> > *the Microsoft-only SMTP extension that popped up a couple of months*
> > *ago as a*
> > *vulnerability.*
> >
> > *Now, *if* it does, it *breaks* something that Microsoft Exchange*
> > *Server does when talking– see– that's the point, protection comes at*
> > *the cost of breaking functionality once you get to the point where*
> > *you've knocked out*
> > *the out-of-band stuff and you're just left with the in-band attacks.*
>
> *I used Cisco's proxying of SMTP as a well-known example of a "security*
> *feature" which breaks legitimate protocol extensions (ESMTP), yet*

That's the point; You stop things (I don't think it really "breaks it," since it should default to HELO instead of EHLO– so "doesn't allow increased functionality" is probably more accurate.) Heck, I try not to run browsers that do ActiveX when I run a browser on a Microsoft OS, that's reduced functionality too– but I'm willing to accept it because it reduces my risk.

Guards with guns stop the free flow of people, and reduce the functionality of a place– but they also reduce the risk if they're doing their jobs– and many places are happy to deploy them.

> *doesn't seem to really improve security, but if you aren't very familiar with it, I won't insist on debating this particular example.*
> :-)

Does it stop the MS-only extensions? In that case it does provide some security value– unless you feel that overflows in SMTP verbs aren't that big a security deal...

I know SMTP-fixup had poor implementation bugs initially, but that still doesn't remove the "able to reduce risk by denying things," it simply speaks to the quality of implementation.

>
> *How about excessive ICMP filtering breaking path MTU discovery?*

Sure it might, but that doesn't mean it doesn't provide security from ICMP attacks. Again, it's a risk/reward calculation– but the blocking reduces risk, at the expense of either operational capability or functionality.

FWIW, "excessive" (which is really trying to paint the landscape) ICMP filtering doesn't have to break PMTU discovery if you filter after you've already lowered the MTU before it hits that router– back when lots of things had ICMP frag overlap problems, I used to "excessively" filter some networks just fine, and the older devices were protected.

Blocking outbound TCP/6667–7002 reduces lots of risk for lots of networks, but it breaks IRC to a lot of networks. That's the name of the game, reducing risk by being more conservative in what you accept, and trading reduced operations and functionality for increased security.

That's still it in a nutshell, block stuff and reduce risk. How much stuff, and how much risk are the practice of security implementation, but the essence remains the same.

Paul

Paul D. Robertson "My statements in this message are personal opinions paul@compuwar.net which may have no basis whatsoever in fact."

--__--__--

Message: 3

Date: Thu, 19 May 2005 17:45:40 -0400 (EDT)

From: "Paul D. Robertson" <paul@compuwar.net>

To: Chuck Swiger <chuck@codefab.com>

Cc: firewall-wizards@honor.icsalabs.com, Martin <marty@supine.com>

Subject: Re: [fw-wiz] A fun smackdown...

On Thu, 19 May 2005, Chuck Swiger wrote:

> *Paul, why *don't* people run their firewalls with a single "deny all"*
> *rule?*
>

Actually, thinking about it, because it's cheaper to just not connect systems that don't need the risk, and you lose the risk of implementation errors in the firewall, configuration errors, and it then takes physical presence to bridge the gap, reducing the rate of attack (which is probably extremely low anyway.)

Now I've got one for you; Why do some people run firewalls with a single "allow all" rule, and what can you do to make that less risky than the "deny all" example?

Paul

-

Paul D. Robertson "My statements in this message are personal opinions paul@compuwar.net which may have no basis whatsoever in fact."

--_--_--

Message: 4

Cc: firewall-wizards@honor.icsalabs.com, Martin <marty@supine.com>

From: Chuck Swiger <chuck@codefab.com>

Subject: Re: [fw-wiz] A fun smackdown...

Date: Thu, 19 May 2005 18:32:11 -0400

To: "Paul D. Robertson" <paul@compuwar.net>

On May 19, 2005, at 5:45 PM, Paul D. Robertson wrote:

>> *Paul, why *don't* people run their firewalls with a single "deny all"*
>> *rule?*

>

> *Actually, thinking about it, because it's cheaper to just not connect*
> *systems that don't need the risk, and you lose the risk of*
> *implementation errors in the firewall, configuration errors, and it*
> *then takes physical*
> *presence to bridge the gap, reducing the rate of attack (which is*
> *probably*
> *extremely low anyway.)*

Right, that's better: there's no need to use a firewall at all for a truly standalone system, those can be set up and updated via CD, without being networked at all.

You only need a firewall when you need to permit some kinds of network traffic.

> *Now I've got one for you; Why do some people run firewalls with a
> single
> "allow all" rule, and what can you do to make that less risky than the
> "deny all" example?*

A firewall with allow-all is simply a router.

I've disabled the firewall on my Linksys BEFS81 broadband router I use at home because the FreeBSD box set up as my DMZ host is set up as a honeytrap. A BSD network stack seems to time out TCP connections after about 10 minutes, if no traffic goes by, but you can get a Windows worm stuck for days if you reply using a 0 window size.

I suspect that using greylisting, honeytraps, teergrubes, and similiar techniques can do a lot to help slow down the spread rates of malware and spam. That's one way of making an "allow all" rule less risky than the "deny all" rule might be. Of course, you have to make sure your honeytrap software is up to the task, which is not as easy as it might seem.

Has anyone else tried setting up several honeytraps across their address space? Have you noticed a difference in connection rates between IP addresses at the far ends of your IP range, compared with honeytrap IP's in the middle?

--

-Chuck

--_--_--_--

Message: 5

Date: Thu, 19 May 2005 18:40:38 -0400 (EDT)

From: "Paul D. Robertson" <paul@compuwar.net>

To: Chuck Swiger <chuck@codefab.com>

Cc: firewall-wizards@honor.icsalabs.com, Martin <marty@supine.com>

Subject: Re: [fw-wiz] A fun smackdown...

On Thu, 19 May 2005, Chuck Swiger wrote:

> > Now I've got one for you; Why do some people run firewalls with a
> > single "allow all" rule, and what can you do to make that less risky
> > than the "deny all" example?

>

> A firewall with allow-all is simply a router.

You'd be surprised at the number of "Yes we have a firewall!"'s I've seen with an allow all...

> I've disabled the firewall on my Linksys BEFS81 broadband router I use
> at home because the FreeBSD box set up as my DMZ host is set up as a
> honeytrap. A BSD network stack seems to time out TCP connections
> after about 10 minutes, if no traffic goes by, but you can get a
> Windows worm stuck for days if you reply using a 0 window size.

>

> I suspect that using greylisting, honeytraps, teergrubes, and similiar
> techniques can do a lot to help slow down the spread rates of malware
> and spam. That's one way of making an "allow all" rule less risky
> than the "deny all" rule might be. Of course, you have to make sure
> your honeytrap software is up to the task, which is not as easy as it
> might seem.

I still don't see that as less risky.

>

> Has anyone else tried setting up several honeytraps across their

Firewall-Wizards: [fw-wiz] UNSUBSCRIBE

> address space? Have you noticed a difference in connection rates
> between IP addresses at the far ends of your IP range, compared with
> honeytrap IP's in the middle?
I haven't, but I know a lot of worms generate addresses to try to infect
with non-random algorithms. Most people I know who do that sort of thing
tend to grab the first bit of traffic, talking enough of whatever protocol
it is to characterize it and tally it up. I'd bet the breakdown by protocol
and malcode instance would be interesting, but it's a heck of a lot of work
to keep it updated.
Paul

-
Paul D. Robertson "My statements in this message are personal opinions
paul@compuwar.net which may have no basis whatsoever in fact."

--_--_--
Message: 6

Date: Fri, 20 May 2005 04:17:11 +0530
From: Devdas Bhagat <devdas@dvb.homelinux.org>
To: firewall-wizards@honor.icsalabs.com
Subject: Re: [fw-wiz] A fun smackdown...
Reply-To: Devdas Bhagat <devdas@dvb.homelinux.org>
On 19/05/05 17:32 -0400, Paul D. Robertson wrote:

<snip>

> >

> > I used Cisco's proxying of SMTP as a well-known example of a
> > "security feature" which breaks legitimate protocol extensions
> > (ESMTP), yet

>

> That's the point; You stop things (I don't think it really "breaks
> it," since it should default to HELO instead of EHLO- so "doesn't
> allow

Yes it does. Minimally, it breaks the requirement that the server advertise
its fully qualified hostname to the remote SMTP client in the greeting.

> increased functionality" is probably more accurate.) Heck, I try not
> to

The increased functionality enhances security by allowing for

1> SMTP AUTH

2> TLS

3> being able to reject before 'data' based on size as offered by the
3> client.

(otherwise you have to accept all the data and that can lead to a DoS).

4> Catching broken spamware and proxies which spew out SMTP protocol
stuff before responses without offering EHLO and explicitly being offered
pipelining.

> run browsers that do ActiveX when I run a browser on a Microsoft OS,
> that's reduced functionality too- but I'm willing to accept it because
> it reduces my risk.

>

> Guards with guns stop the free flow of people, and reduce the
> functionality of a place- but they also reduce the risk if they're
> doing their jobs- and many places are happy to deploy them.

>

> > doesn't seem to really improve security, but if you aren't very
> > familiar with it, I won't insist on debating this particular
> > example.

> > :-)

>

> Does it stop the MS-only extensions? In that case it does provide
> some security value- unless you feel that overflows in SMTP verbs
> aren't that big a security deal...

But those could be stopped by a ESMTP speaking defensive proxy as well.

Devdas Bhagat

Firewall-Wizards: [fw-wiz] UNSUBSCRIBE

--_--_--

Message: 7

Cc: firewall-wizards@honor.icsalabs.com, Martin <marty@supine.com>

From: Chuck Swiger <chuck@codefab.com>

Subject: Re: [fw-wiz] A fun smackdown...

Date: Thu, 19 May 2005 18:58:57 -0400

To: "Paul D. Robertson" <paul@compuwar.net>

On May 19, 2005, at 6:40 PM, Paul D. Robertson wrote:

>> A firewall with allow-all is simply a router.

>

> You'd be surprised at the number of "Yes we have a firewall!"'s I've

> seen

> with an allow all...

Look on the bright side, they have a lot of unused capability where they could improve their security, if only someone showed them how to use it.

Sounds like a happy consulting opportunity. :-)

>> I suspect that using greylisting, honeytraps, teergrubes, and

>> similiar techniques can do a lot to help slow down the spread rates

>> of malware and spam. That's one way of making an "allow all" rule

>> less risky than the "deny all" rule might be. Of course, you have to

>> make sure your honeytrap software is up to the task, which is not as

>> easy as it might seem.

>

> I still don't see that as less risky.

Is it easier to defend against a known attack then against an unknown one?

>> Has anyone else tried setting up several honeytraps across their

>> address space? Have you noticed a difference in connection rates

>> between IP addresses at the far ends of your IP range, compared with

>> honeytrap IP's in the middle?

>

> I haven't, but I know a lot of worms generate addresses to try to

> infect

> with non-random algorithms. Most people I know who do that sort of

> thing

> tend to grab the first bit of traffic, talking enough of whatever

> protocol

> it is to characterize it and tally it up. I'd bet the breakdown by

> protocol and malcode instance would be interesting, but it's a heck of

> a

> lot of work to keep it updated.

Computers are good at logging and keeping track of the statistics. The problem is understanding what all of the noise means and presenting it to the user in a fashion which helps them make decisions.

--

-Chuck

--_--_--

Message: 8

Date: Thu, 19 May 2005 19:01:37 -0400 (EDT)

From: "Paul D. Robertson" <paul@compuwar.net>

To: Devdas Bhagat <devdas@dvb.homelinux.org>

Cc: firewall-wizards@honor.icsalabs.com

Subject: Re: [fw-wiz] A fun smackdown...

On Fri, 20 May 2005, Devdas Bhagat wrote:

> On 19/05/05 17:32 -0400, Paul D. Robertson wrote:

> <snip>

> > >

> > > I used Cisco's proxying of SMTP as a well-known example of a

> > > "security feature" which breaks legitimate protocol extensions

> > > (ESMTP), yet

> > >

Firewall-Wizards: [fw-wiz] UNSUBSCRIBE

> > That's the point; You stop things (I don't think it really "breaks
> > it," since it should default to HELO instead of EHLO- so "doesn't
> > allow
>
> Yes it does. Minimally, it breaks the requirement that the server
> advertise its fully qualified hostname to the remote SMTP client in
> the greeting.
I'd read Chuck's message to say that it doesn't allow ESMTP, which is
different than breaking it, as you can simply downgrade to SMTP.
>
> > increased functionality" is probably more accurate.) Heck, I try
> > not to
>
> The increased functionality enhances security by allowing for
> 1> SMTP AUTH
> 2> TLS
> 3> being able to reject before 'data' based on size as offered by the
> 3> client.
> (otherwise you have to accept all the data and that can lead to a
> DoS).
> 4> Catching broken spamware and proxies which spew out SMTP protocol
> stuff before responses without offering EHLO and explicitly being
> offered pipelining.
>
I'm not arguing that ESMTP doesn't have useful features, I'm saying that not
allowing it is a valid security control, as it increases complexity (SSL
layer in TLS? Auth password guessing...) and specifically if it stops the
last Exchange bug, then it's value may come to be a lot greater than
previously thought for those folks who use SMTP-fixup and Exchange
(editorial comments narrowly avoided.)
Actually, you don't have to accept all the data, you can simply close the
connection at N bytes, which you'd have to do if the client lied anyway.
Also, I've seen the same spew in "legitimate" applications (specifically
Delphi controls that couldn't do SMTP correctly,) which is generally where
you get the most flack for adding security controls (breaks "needed
functionality.")
> > run browsers that do ActiveX when I run a browser on a Microsoft OS,
> > that's reduced functionality too- but I'm willing to accept it
> > because it reduces my risk.
> >
> > Guards with guns stop the free flow of people, and reduce the
> > functionality of a place- but they also reduce the risk if they're
> > doing their jobs- and many places are happy to deploy them.
> >
> > > doesn't seem to really improve security, but if you aren't very
> > > familiar with it, I won't insist on debating this particular
> > > example.
> > > :-)
> >
> > Does it stop the MS-only extensions? In that case it does provide
> > some security value- unless you feel that overflows in SMTP verbs
> > aren't that big a security deal...
>
> But those could be stopped by a ESMTP speaking defensive proxy as
> well.
Which doesn't mean the downgrade wouldn't be protective.
Paul

Paul D. Robertson "My statements in this message are personal opinions
paul@compuwar.net which may have no basis whatsoever in fact."

Firewall-Wizards: [fw-wiz] UNSUBSCRIBE

firewall-wizards mailing list firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
End of firewall-wizards Digest

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>