

Re: How to do rDNS. WAS: RE: educating rDNS violators

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-08/0279.html>

From: Chris Olave (*chrisfocus_at_saber.net*)

Date: 08/25/04

To: "Ferino Mardo" <RMardo@ALJOMAIHBEV.com>

Date: Tue, 24 Aug 2004 23:55:53 -0700

It's done in the DNS server.

As a spam prevention measure, a lot of end-user Internet providers are firewalling the SMTP port (25) to the rest of the world. This is a spam prevention measure for attempting to reduce spam from end-nodes or potential compromised spam-zombies. A lot of providers are getting the idea that all mail sent from their customers should be routed through their hosts so they will have all the proper logs. Users that are hosting their own mail servers should setup use their ISP's mail server as a hub (before it's a requirement), if they choose to run their own equipment. A lot more providers are becoming very security conscious and attempting to help the rest of the world by reducing the potential for their services to be abused. A lot of providers are going to the extent to firewall commonly used virus ports and things of that nature; it's not long before it's a common practice to close port 25 to the world.

Using your own mail server as a slave to the ISP's mail server will add another hop to the headers, yes; but it is very rare that you will find an ISP block a message for "Too many hops" (unless there's a mail loop). Typically providers will allow 10-15 hops which is usually more than enough unless a lot of internal hosts route mail around (in which case their hop-count would be raised anyway)

As a common courtesy to other mail server administrators, a forward (A) and a reverse (PTR) should be in DNS for any host delivering to a remote network. It's nice to have PTR records so that a DNS will be able to resolve a hostname from IP; it will give you a domain name to WHOIS if you need more/contact information.

If I had the smarts, (I do, I'm just incredibly lazy; I have the ideas, someone else can write the code...) I would write a ruleset that would check if the "From:" domain was MX-able. I know there are configurations for checking to make sure the domain exists in DNS; however, I'm not sure if there are any pre-written ones to do MX validation.

SecurityFocus BASICS: Re: How to do rDNS. WAS: RE: educating rDNS violators

If anyone knows of pre-written MX checks or local user validation (on the "From:" address), please let us know. Our problem now is that our domain is being spoofed in spam, however the generated username prefixed to our domain doesn't exist. It would be nice to check to make sure it was a true local user (real user/aliases/virtusertable/etc); I think that would cut a *significant* amount of spam.

Anyone with this kind of experience?

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

From: "Ferino Mardo" <RMardo@ALJOMAIHBEV.com>

To: "Chris Olave" <chrisfocus@saber.net>;

<security-basics@securityfocus.com>

Sent: Tuesday, August 24, 2004 11:26 PM

Subject: How to do rDNS. WAS: RE: educating rDNS violators

>
> *This is a nice read. Just like to ask how does one implement rDNS from
> the mail server? Or is it done from the DNS server?*

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

> > *From: Chris Olave [mailto:chrisfocus@saber.net]*

> > *Sent: Tuesday, August 24, 2004 6:21 AM*

> > *To: SMiller@unimin.com; security-basics@securityfocus.com*

> > *Subject: Re: educating rDNS violators*

> >
> >
> > *Our previous mail server setup included refusing all messages
> > coming from non-resolvable IP addresses. We had toyed with
> > the idea of imposing a full DNS check (forward to reverse
> > matching reverse to forward), however we decided that it
> > refused too much potentially-legit mail, we only allowed it
> > for about a half hour.*

> >
> > *We had the rDNS requirement imposed for about two years and
> > never had a problem with it. Friends and family emailing our
> > customers would get a customized refusal saying "hostname
> > lookup failed"; they seamlessly would forward it on to their
> > provider who would eventually fix the problem. We imposed
> > this restriction and noticed a fair amount of junkmail
> > missing from our inboxes the next morning.*

> >
> > *Another way to catch a fair amount of spam is to require that
> > the "From:" addresses on messages be MX-able. This will only
> > catch the small bit of spam that hasn't caught up to the rest
> > of the world (using fake domains). Newer spam methods include
> > using a fake address "@yourdomain.com"; you could write a
> > ruleset that will check to see if the "From:" is a valid
> > local user (only if it's a local domain, obviously) and*

Re: How to do rDNS. WAS: RE: educating rDNS violators

SecurityFocus BASICS: Re: How to do rDNS. WAS: RE: educating rDNS violators

> > *refuse to deliver the message based on the "From:" not being
> > a true local user. This will catch a fair amount of spam as well.*
> >
> > *Have you looked into using services such as the MAPS RBL, DUL
> > or other lists? We used these for a while and they seem to
> > catch a good amount, but not nearly enough spam.*
> >
> > *We eventually decided to go with a "middle-man" mail filter.
> > We pointed our MX records to the filter then the filter would
> > forward mail to our SMTP server. Then we had the problem of
> > spammers directly delivering mail to our server (ignoring
> > MX). Then we had to impose restrictions for our mail filter
> > to be "OK" to deliver mail but no one else. We are soon
> > going to be changing our refusal message from "Access denied"
> > to "Please honor our MX records and we'll accept your mail."
> >
> > *Our customers have not voiced any kind of displeasure. If
> > they do, we will simply have to tell them the remote end
> > needs to honor our MX records; servers not abiding by it are
> > not abiding by SMTP protocol in which case there's probably a
> > reason they are trying to bypass the filter.*
> >
> >
> > *Good luck!*
> >
> > ----- Original Message -----
> > *From: <SMiller@unimin.com>
> > To: <security-basics@securityfocus.com>
> > Sent: Wednesday, August 18, 2004 2:49 PM
> > Subject: educating rDNS violators*
> >
> >
> > > *Our mail administration group recently implemented blocking of all
> > > incoming
> > > messages from domains that cannot be resolved via reverseDNS, for
> > > purposes of spam prevention. Of course, there are quite a
> > > number of
> > > legitimate business contacts who do not have rDNS properly
> > > configured.
> > > Assuming that the rDNS criterion remains, the question
> > > becomes one of
> > > who will notify and/or educate the sender(s) about this issue. The
> > > only time-efficient
> > > way
> > > that I can think of to do this would be to have instructions and
> > > references
> > > in the body of the bounce message itself. Anyone tried that?
> > > Results? Other suggestions? Thanks in advance.*
> > >
> > > *Scott*
> > >*

>>>
>>>
>>

>>> -----
>> -
>>> *Computer Forensics Training at the InfoSec Institute. All
>> of our class
>> sizes
>>> are guaranteed to be 12 students or less to facilitate one-on-one
>>> interaction with one of our expert instructors. Gain the in-demand
>>> skills
>> of
>>> a certified computer examiner, learn to recover trace data
>> left behind
>>> by fraud, theft, and cybercrime perpetrators. Discover the
>> source of
>>> computer crime and abuse so that it never happens again.*
>>>
>>>
>> [http://www.securityfocus.com/sponsor/InfoSecInstitute_security
> -basics_040817](http://www.securityfocus.com/sponsor/InfoSecInstitute_security-basics_040817)
>>

>> -----
> --
>>
>
>
>

> ----
> *Computer Forensics Training at the InfoSec Institute. All of our class
> sizes are guaranteed to be 12 students or less to facilitate one-on-one
> interaction with one of our expert instructors. Gain the in-demand
> skills of a certified computer examiner, learn to recover trace data
> left behind by fraud, theft, and cybercrime perpetrators. Discover the
> source of computer crime and abuse so that it never happens again.*
>
> http://www.infosecinstitute.com/courses/computer_forensics_training.html
>

> -----
>
>

Computer Forensics Training at the InfoSec Institute. All of our class sizes are guaranteed to be 12 students or less to facilitate one-on-one interaction with one of our expert instructors. Gain the in-demand skills of a certified computer examiner, learn to recover trace data left behind by

SecurityFocus BASICS: Re: How to do rDNS. WAS: RE: educating rDNS violators

fraud, theft, and cybercrime perpetrators. Discover the source of computer crime and abuse so that it never happens again.

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