

Re: IIS5 Passive FTP Networking problem (long)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-12/0202.html>

From: WinGuy (no_spam_at_nomail.bot)

Date: 12/14/04

Date: Tue, 14 Dec 2004 15:05:57 GMT

"Bernard" <qbernard@hotmail.com.discuss> wrote in message
news:e9dWS5a4EHA.2540@TK2MSFTNGP09.phx.gbl...

...

>> *The first problem is that I can not tell by the below listing if that*
>> *5555-5700 port range is being respected when the server responds with*
>> *"Entering Passive Mode (192,168,1,100,21,188)". I see that the IIS IP*
>> *address of 192.168.1.100 is represented there, and that the command port*
>> *is 21, but I don't see how "188" is supposed to represent a data port*
>> *within the range of 5555-5700.*

>

> *Yes, it is within the port range, to calculate it. you take the last two*

> *'numbers'*

> *21 * 256 + 188 = 5564*

> *detail -*

> *Information About the IIS File Transmission Protocol (FTP) Service*

> <http://support.microsoft.com/?id=283679>

Oh! Thanks! I fell for an improper assumption. In the server response
67.115.67.162 192.168.1.252 FTP Response: 227 Entering Passive Mode
(192,168,1,100,21,188)

I improperly assumed that the "21" referred to the FTP command port. I
didn't realize that it represented the high-byte of a decimal representation
of a 2-byte value, in high+low format instead of the (in code programming)
traditional low+high format. Pure coincidence! But I should have realized
that the FTP control port 21 is always used regardless of if active or
passive mode is implemented, and thus the control port 21 (defined by RFC)
never needs to be specified (and in fact is not specified).

That leaves me only with the client side Microsoft Base Station (MBS) router
client response of

192.168.1.252 Broadcast ARP Who has 192.168.1.100? Tell 192.168.1.252
being the sole remaining problem; keeping in mind that 192.168.1.252 is one
of many LAN clients behind the MBS that has a static public WAN address of
67.115.67.161, while 192.168.1.100 is the IIS box behind the Linksys v2
router that has a static WAN address of 67.115.67.162. The ARP broadcast
would also occur for any other client on the internet that is behind a
router, since it wouldn't know who 192.168.1.100 is. Worse, if the LAN that

hosts the box that issues that ARP happens to have a box with a 192.168.1.100 address then an improper LAN network condition would exist! The client side LAN problem is not constrained to my own LAN, it also occurs for any client that is hiding behind a router (such as many do when connecting to IIS via internet).

That ARP is a direct result of the IIS5 FTP Service response (it is not a response from the router):

```
67.115.67.162 192.168.1.252 FTP Response: 227 Entering Passive Mode (192,168,1,100,21,188)
```

where IIS identifies itself as being 192.168.1.100 instead of it spoofing itself as being 67.115.67.162. If it did the spoof (if IIS could be configured to respond like that) then the Linksys router would forward the ports just fine to IIS (which is truly assigned a LAN address of 192.168.1.100) and passive FTP would work.

I don't know if it's true or not, but a tech at Linksys said that version 3 firmware for the BEFSR41 router correctly translates the LAN address into its own WAN address in the packet that IIS sends, and the ARP is thus avoided. But version 2 firmware can not be upgraded to version 3, so I can only use the very latest release of the version 2 firmware (which I do) from Linksys and it obviously does not do the needed IP address translation.

This means I have to do a "fix" by somehow configuring IIS FTP Service to spoof the WAN address of its router in its response to a request to use passive mode, or do away with the router entirely (and the hardware based security benefits that it provides) and give IIS a real (instead of spoofed) public WAN address. If I toss the router then I have to replace it with an transparent IP-less firewall called "IP-Filter", which comes with FreeBSD, if I want to take the majority of firewall load off of the server CPU (primarily to protect it from a DoS, as well as to take the load off of its own software based firewalls BlackIce and ZAP --- yes, I run 2 firewalls on the IIS box!) I don't see how I can make IIS do the spoof, though, as the IIS5 FTP Service obviously can not be configured to truly have the same WAN address as the one that is used by its Linksys router. But I'd really like to not have to use IP-Filter on FreeBSD, either! It's hard to maintenance.

This all is not a problem with active FTP, since the routers properly translate and forward things for ports 20 and 21. But (most) routers do not do the same for passive FTP data ports, although usage of the control channel only (port 21) does still get properly translated and only the passive data channel gets munged. Active FTP works fine. But most people behind a router would use passive mode, if for no other reason than IE6 (in its Advanced settings) suggests that one should do so for DSL and router based networks! So, I need to tell IIS5 how to spoof its FTP Service IP address, or I need to toss the router.

Anyone know if its possible to make IIS FTP Service do the necessary spoof? Or is there some other solution without having to toss the Linksys router?

Winguy