

Re: OT udp port 138 BROWSER traffic

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2004-01/0006.html>

From: Newsbox (newsbox_at_MAPS_ON_customers-of-adelphia.org)

Date: 01/01/04

Date: Thu, 01 Jan 2004 02:52:41 -0500

On Wed, 31 Dec 2003 14:21:35 -0500, BM wrote:

> *Newsbox wrote:*

>> *On Tue, 30 Dec 2003 15:49:55 -0500, Brad Olin wrote:*

>>

>>

>>> *On Tue, 30 Dec 2003 15:19:40 -0500, Newsbox*

>>> *<newsbox@MAPS_ON_customers-of-adelphia.org> wrote:*

>>>

>>>

>>>> *So my question is, what kind of security risk, if any, does the NT workstation run by having this BROWSER service running on a public network? Is there ever a good reason or justification to run that publicly, or is that not recommended? I'm just looking for some kind of general frame of reference.*

>>>>

>>>>

>>>>

>>>> *There isn't really a risk to your linux firewall box, but there are potential problems with people outside the firewall looking at disk info that resides on windows boxes that are inside your firewall. The best policy is just to drop all ms browser traffic. The below netfilter rules will do the trick. Please know that you will need to adjust these if you want samba to work on the inside nic of your firewall.*

>>>>

>>>>

>>>> *# drop all Microsoft peer-to-peer networking traffic /sbin/iptables -A INPUT -p udp --dport 137:138 -j DROP /sbin/iptables -A INPUT -p tcp --dport 139 -j DROP*

>>>>

>>>>

>>>>

>>>>> *Also while we are off topic, is there any reason to believe that this kind of BROWSER broadcast would make a properly configured router stumble? (It was a broadcast packet, 243 bytes long.) This is a Cisco router but that is all I know about it. Is there a better or more meaningful way to test, rather than using ping?*

>>>>>

>>>>

>>>>

>>>Take a look at traceroute and nmap... there are lots of good tools and
>>>your question is a bit vague, so I'm uncertain how to best answer this
>>>one. Post again, with more specifics, if that's not what you were
>>>looking for.

>>>

>>>

>>>Brad

>>

>>

>> Thanks Brad,

>>

>> I seldom power up a Windows OS any more, and it is even more rare that
>> I send or receive any public network traffic from them. I believe that
>> at some point I have gone into each Windows machine and disabled
>> peer-to-peer networking, but I would check that again before
>> connecting, even behind the Linux firewall, "just in case".

>>

>> Thanks for the nice, specific firewall rules. – I always like to triple
>> check anything I do with iptables, because it always look to me as if
>> it might be easy to make a mistake if not careful. I have been using
>> rules that are based on the ones that the "Firestarter" script
>> generated, with a few extra rules added, and I have checked that all
>> these rules are working with several scanning services (grc.com and
>> nessus, if I remember correctly, among some others.) The ports 137–139
>> are properly closed (stealthed") last time I checked, and I'll check
>> again. Thanks very much.

>>

>> The situation is frankly that I am kind of running out of time to be
>> patient with a very spotty (intermittent) dsl connection, and I'm at
>> the point of changing dsl providers. I have alternate dial-up service
>> that works fine, but uses up the Lady's voice line, naturally :(The
>> dsl issues extend from at least June, and I could say more, but won't.

>>

>> It occurred to me that, like many other businesses today, they may be
>> short-handed and may not have the time or expertise to track all the
>> issues that are interfering with my connection at their end. And that
>> if I could tell them exactly what some of the causes of the problems at
>> their end specifically were, there would be a higher probability that
>> they would be quickly corrected.

>>

>> To this end I have been periodically checking the connection between my
>> firewall/router and their gateway, which is a cisco router. This was
>> all going on before the major emergency Cisco router IOS upgrade the
>> week of July 15, 2003. This past week I began using Ethereal network
>> traffic analyzer to see if I could detect anything unusual happening at
>> those times that my traffic was being ignored. And I should say that
>> this is not a signal issue, and it is not at my end. What is actually
>> happening is the router (gateway) is simply ignoring my traffic, while
>> occasionally sending me traffic of its own at the same time.

>>
>> *It was never my intention to publicly embarrass them, and still is not,
>> and that is probably why I was somewhat vague in my question. I
>> apologize to you for that. I have found some things that were
>> happening concurrent with the connection problems, that seemed so
>> entirely wrong that even I as a home user with no formal computer
>> science training, had to know they were wrong. That router was
>> broadcasting ARP requests to find an IP address that was in fact its
>> own interface address, and that was causing loss of ping replies. I
>> told them and it appears to have stopped now. There were ARP requests
>> coming at me for 10.xxx.xxx.xxx addresses, and that was causing the
>> gateway router to ignore my traffic and stop replying. I told them and
>> it appears to have stopped now.*
>>
>> *I am still losing traffic, as measured by ping, however I am also
>> losing apparently just about any kind of traffic that I happen to be
>> sending when their router develops some problem. That kind of problem
>> seems to be occurring when it gets a MS BROWSER announcement as I
>> described. I know that 10... addresses do not belong on a public
>> network. But I do not know if BROWSER announcements belong on the
>> public network, or what the risks might be to the individual(s) who are
>> using those NT workstations. If they are inadvertently exposing
>> themselves to unwanted security risks by running this service (if
>> that's what it is called), and if that same traffic is interfering with
>> my connection, then maybe the best answer is to just have them disable
>> that service.*
>>
>> *Another apparent hurdle is that the ISP doesn't want to acknowledge
>> that losing some ping replies is anything to be concerned about, and I
>> would have to agree, in principle. But they do respect the seriousness
>> of losing DNS. I have a script that I wrote that uses ping and writes
>> a log of each connection loss. If I knew how to do that same thing,
>> but using say DNS requests and replies they would be more willing to
>> take the issue seriously. I don't know how to do this with say DNS or
>> some other, higher priority protocol.*
>>
>> *And I don't know serious a security issue it would be for a MS Windows
>> NT workstation user to be running BROWSER announcements and possibly be
>> unintentionally and unknowingly opening their computer to the public.
>> They might appreciate a "heads-up" and the chance to protect
>> themselves. Possibly?*
>>
>> *This whole connection issue, one way or another, is not going to go on
>> very much longer. I work from home and I need a reliable connection. I
>> apologize again for being somewhat vague in my original post. And I
>> thank you very much for your kind and knowledgeable suggestions and
>> offer of help. It is truly appreciated.*
>>
>> *Best wishes.*
>>
> Newsbox –

>
> *I'm assuming the DSL is home use. If this is so then it may be simple*
> *to figure ou the problem. I had spotting DSL connection as well. In*
> *short, it was a BAD filter that was not doing it's job.*
>
> *Disconnect all your phones form yoru house, and leave the DSL*
> *connectes... see if you still have a problem, if you don't add a phone,*
> *and try using the DSL, then keep adding a phone (one by one) and see if*
> *it acts up. if so, it is most likely the filter. Remove that phone,*
> *and try any remaining, removing bad filter/phone combos, untill you weed*
> *all of them out. then , go buy new filters (Best buy, on-line)your*
> *call.*
>
> *My kitchen one was bad. Had to get it replaced, but my DSL is fine now.*
>
> *Hope that helps, and good luck.*
>
> *Bill*

Hey Bill, Thanks!

Many thanks for the kindness to take your time and share your experience. Yes, it is a home dsl and those phone filters can be a problem, I know. I wish I had had your helpful advice in February, when I learned about the filters, the hard way. Only after discovering the (voice) phone line interference myself did anyone at the ISP acknowledge that, yes, of course, I needed them. I guess I was supposed to know that from somewhere else, because they didn't tell me that anywhere until I asked.

I installed the filters and did essentially the checks that you suggested. The phone in the kitchen is wall mounted, and I had to wire in a new jack in the basement to get the filter for that one installed.

In June, I did that whole check again when the service got really bad. Turns out that it was a Cisco router DOS vulnerability, that was in fact giving me a denial of service. But I didn't find out about that until about July 16 or 17. By then I had rewired the house with new CAT3 cable, and run a dedicated CAT3 cable directly from the NID to the dsl modem. None of that helped at all with the major problem, until the Cisco IOS upgrades were completed during the week of July 15.

And, you know, I think it is a pretty reasonable expectation that when a business lies to its customers in the face of direct evidence and questioning, that the next time it happens, the customer (like me) just doesn't believe them anymore. It's like the old saying "Fool me once, –shame on you. Fool me twice, –shame on me." I need to depend on independently verifiable facts as bases for any decisions that I make, because I can't believe the people whom I am paying to provide my Internet connection. Unfortunately, that is the state of trust in businesses today in general, and in the Internet community in particular. And I would add that this is not just a matter of some passing annoyance or loss of

service at unpredictable and critical times, but that there were security issues involved that were not publicized, that go well beyond DOS. Probably 'nuff said about that, except to add that I feel fully justified in chasing this down to the very last detail that I can, and by any means necessary. Cisco routers probably run 95% of the Internet, worldwide, and that's just the "tip of the iceberg". Cisco may be well justified in hiding deficiencies, but are no less to blame for worldwide security vulnerabilities than Microsoft. The local ISP's can try, but are really not equipped to deal with these widespread issues in general. And, incidentally, I did get an explicit acknowledgment from the ISP the these problems were not in my computer, or at my end of the line.

There has been work done, and there have been service improvements in the past week. And while I am still losing some ping packets, I have not yet been able to document losing any higher priority traffic, and have not noticed that in my usage of the past couple of days. Perhaps the underlying problems have been resolved, and I will continue to try to improve my skills in monitoring the connection.

As I stated in my original post,
>>>>> [...] *(The loss is not at my end.)* [...]

Your kind and clearly articulated suggestions would have been exactly what I needed about 11 months ago, and will still be valuable to newer dsl users for as long as the archives are accessible, if they are able to find them. Your forthcoming presentation of immediately useful and relevant information is exactly in the spirit and nature of what made the Internet a great multiplier for personal productivity. I sincerely appreciate your help.

Thanks again, and all good wishes for the New Year.

Happy New Year !

--
Remove the backwards _NO_SPAM for e-mail
... Trying to cut down on the backwards NEWS virus mail
Thanks !!