

Re: Home firewall Hits

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-11/0065.html>

From: Tijn DULLERS (*Tijn.DULLERS_at_dhl.com*)

Date: 11/04/03

Date: Tue, 04 Nov 2003 11:29:20 +0100

To: "Preston Tony" <Tony.Preston@acs-inc.com>

Hi,

Port 162 UDP = SNMP traps.

Did you configure your wireless router to send SNMTP traps to your workstation PC ?

Or do you have SNMP enabled on the Wireless router at all ?

Preston, Tony wrote:

>I am hoping someone here can explain what I am seeing on my home network.

>I use Kerio's tiny personal firewall and Windows ME. I have everything up

>to date with the latest patches.

>

>This is my home network and something strange is happening. The

>configurations is

>

>

> [cable modem] <----> [Linksys Wireless Router] ~~~ [Windows ME W/
>firewall]

>

>

>From reading the firewall log, I would think that my router is continuously

>hitting

>Port 162 with a UDP message. The odd thing is that it is doing this by

>using an

>incrementing port from 192.168.1.1, I see many of these every day, it is

>continuous.

>

>I have the latest firmware from linksys, the firewall is rejecting all the

>packets.

>

>While I am an experienced programmer, I do not have alot of network

>experience, probably

>I would classify myself as knowing enough to be dangerous...:)

>

>The activity is at a moderate rate from a couple per second to one every 20

SecurityFocus BASICS: Re: Home firewall Hits

>seconds. If it
>is some sort of attack attempt it is using a randomized delay between
>packets.
>
>Here is a summary of the hits.
>
>[30/Oct/2003 23:53:48] Rule 'Packet to unopened port received': Blocked: In
>UDP,
> 192.168.1.1:40826->localhost:162, Owner: no owner
> thru
> 192.168.1.1:40899->localhost:162, Owner: no owner
>
>
>I do see other "hits" which are much less frequent which are an occasional
>hit here or
>there, I am not as concerned about these, but would be curious if anyone has
>ideas about
>why they occur. The first one, I might see one or two a day. The second
>one would
>show up in sets of 5-10, maybe a couple of times a day.
>
>[30/Oct/2003 23:53:56] Rule 'TCP ack packet attack': Blocked: In TCP,
> 207.46.197.121:80->localhost:1452, Owner: no owner
>
>[31/Oct/2003 00:00:02] Rule 'Packet to unopened port received': Blocked: In
>UDP,
> 0.0.0.0:68->localhost:67, Owner: no owner
>
>Anything here I should be concerned with??
>
>I am hoping someone here can explain what I am seeing on my home network.
>I use Kerio's tiny personal firewall and Windows ME. I have everything up
>to date with the latest patches.
>
>The configurations is:
>
> [cable modem] <-----> [Linksys Wireless Router] ~~~ [Windows ME W/
>firewall]
>
>
>From reading the firewall log, I would think that my router is continuously
>hitting
>Port 162 with a UDP message. The odd thing is that it is doing this by
>using an
>incrementing port from 192.168.1.1, I see many of these every day, it is
>continuous.
>
>I have the latest firmware from linksys, the firewall is rejecting all the
>packets.
>
>While I am an experienced programmer, I do not have alot of network

Re: Home firewall Hits

SecurityFocus BASICS: Re: Home firewall Hits

>experience, probably
>I would classify myself as knowing enough to be dangerous...:)
>
>The activity is at a moderate rate from a couple per second to one every 20
>seconds. If it
>is some sort of attack attempt it is using a randomized delay between
>packets.
>
>Here is a summary of the hits.
>
>[30/Oct/2003 23:53:48] Rule 'Packet to unopened port received': Blocked: In
>UDP,
> 192.168.1.1:40826->localhost:162, Owner: no owner
> thru
> 192.168.1.1:40899->localhost:162, Owner: no owner
>
>
>I do see other "hits" which are much less frequent which are an occasional
>hit here or
>there, I am not as concerned about these, but would be curious if anyone has
>ideas about
>why they occur. The first one, I might see one or two a day. The second
>one would
>show up in sets of 5-10, maybe a couple of times a day.
>
>[30/Oct/2003 23:53:56] Rule 'TCP ack packet attack': Blocked: In TCP,
> 207.46.197.121:80->localhost:1452, Owner: no owner
>
>[31/Oct/2003 00:00:02] Rule 'Packet to unopened port received': Blocked: In
>UDP,
> 0.0.0.0:68->localhost:67, Owner: no owner
>
>Anything here I should be concerned with??
>
>
>

>Forum Systems PRESIDIO: PGP / XML GATEWAY APPLIANCE
>The Presidio integrates PGP data encryption and XML Web Services security to
>simplify the management and deployment of PGP and reduce overall PGP costs
>by up to 80%.
>FREE WHITEPAPER & 30 Day Trial -
>http://www.securityfocus.com/sponsor/ForumSystems_security-basics_031027

>
>
>

SecurityFocus BASICS: Re: Home firewall Hits

- application/x-pkcs7-signature attachment: S/MIME Cryptographic Signature