

Re: [fw-wiz] udp port 0

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2008-02/msg00003.html>

- *From:* "Darden, Patrick S." <darden@xxxxxxxx>
 - *Date:* Tue, 5 Feb 2008 08:21:26 -0500
-

I think you are right. udp 0 is used variously as

next available port (dynamic port assignment)for some Unices
dos attack on early version of cp fw l

Officially, it is reserved under IANA as an unused port.

I would check the OS of the sending and receiving machines. If they
are some flavor of Unix then you could content inspect for protocol
to see if the socket is legitimate.

--Patrick Darden

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

From: firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
[\[mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx\]](mailto:firewall-wizards-bounces@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)On Behalf Of
shadow floating
Sent: Monday, February 04, 2008 12:01 PM
To: firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Subject: [fw-wiz] udp port 0

Hi list

i keep getting logs from my IOS router 12.4 T about denying udp packet
ip a.a.a.a (0) --> b.b.b.b (0)
i kept googling about udp port zero and it's apperantly not used , at
least legitimately. I also inspected the traffic from the logged ip
address via wireshark and it never captures and udp packet with src or
dst port 0, but i still get these logs all day long.
anyone got idea about what it? is it some kind like udp tracerouting ?
thanks alot

regards,

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

Re: [fw-wiz] udp port 0

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>