

RE: ICMP/UDP flood

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-05/0064.html>

From: VonGrebe, Chris (*cvongrebe_at_Intrado.com*)

Date: 05/07/04

Date: Fri, 7 May 2004 12:18:30 -0600

To: <wjburgos@white-bear-productions.com>, <security-basics@securityfocus.com>

Bill,

The UDP destination port is 53, the DNS port. These look like normal DNS operation to me, your firewall is probably your internal DNS server, and when it can't resolve an address it then queries the upstream DNS server for resolution.

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

From: Bill Burgos [mailto:wjburgos@white-bear-productions.com]

Sent: Wednesday, May 05, 2004 7:59 PM

To: security-basics@securityfocus.com

Subject: ICMP/UDP flood

Greetings Security Focus,

I recently have been receiving log messages from my router with the following message:

2004-05-02 00:40:03 - ICMP Flood - Source:192.168.X.XX ,0,LAN -
Destination:2XX.2XX.XX.X,0,WAN

also:

2004-05-06 10:25:27 - UDP Flood - Source:192.168.X.XX
,45544,LAN - Destination:2XX.2XX.XX.X,53,WAN

The Source is coming from my firewall box (192.168.X.XX) and the Destination is a DNS server on the Internet (2XX.2XX.XX.X).

I have grepped the logs from internal machines and the firewall for the DNS server address with no results.

My setup:

Internet

|

RE: ICMP/UDP flood

SecurityFocus BASICS: RE: ICMP/UDP flood

Router



||
Firewall DMZ server (web server)

|
LAN

The Router is a Planex, the firewall is a PC running RedHat 7.2, the DMZ is Debian.

The other LAN machines are a combo of Linux and one Windows machine, all behind the firewall. The messages started while I was out of the house and the Windows machine was offline.

My questions are:

Should I be worried about this?

If the flood is coming from the firewall, is it compromised? can I verify it in a log?

Any ideas would be a great help.

Thanks in advance

Bill

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html