# Re: UDP Port 7 − trying to understand

***Source:*** http://www.derkeiler.com/Newsgroups/comp.security.misc/2006−05/msg00229.html

- *From*: ibuprofin@xxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
- *Date*: Thu, 25 May 2006 14:59:01 −0500

On 25 May 2006, in the Usenet newsgroup comp.security.misc, in article <1148556060.006861.305160@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Java and Swing wrote:

> I understand that UDP port 7 is typically used to run echo.

0792 Internet Control Message Protocol. J. Postel. September 1981.
(Format: TXT=30404 bytes) (Obsoletes RFC0777) (Updated by RFC0950)
(Also STD0005) (Status: STANDARD)

0862 Echo Protocol. J. Postel. May 1983. (Format: TXT=1237 bytes)
(Also STD0020) (Status: STANDARD)

TCP and UDP echo is extremely rare − most systems to not have the client needed to create an echo request, and fewer still have the echo server enabled. The "ping" you are used to is the ICMP Type 8 packet, and has nothing to do with TCP or UDP.

> What I am trying to understand is how, by sending numerous packets to port 7, is this an attack? i.e. how does it cause a problem

Doesn't look any more of a problem than the average port scan. The remote sends a data packet to port 7 on this system. Nothing is listening, so the network stack sends back a RST (or ICMP Type 3 Code 3) − end of conversation.

On 25 May 2006, in the Usenet newsgroup comp.security.misc, in article <1148557260.317929.48840@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, "Java and Swing" <codecraig@xxxxxxxxx> continued:

> ...for example. I understand that if you were to send numerous packets to the broadcast address of a network using UDP on port 7...you could potentially cause the network to be flooded, as all the computers on that network would "echo" what they saw on UDP port 7.

The only thing that would happen is that there _COULD_ be a bunch of RST packets in reply. Just tried it here − _none_ of the systems on the LAN responded. Now, if you did the same thing with an ICMP ping, you may get a bunch of systems trying to reply. However, some operating systems (windoze being one) _ignore_ ICMP pings to a broadcast address. Other systems may be configured to ignore just broadcast pings, or all pings. The reason is simple − l33t wankers have discovered it is possible to waste resources (network bandwidth) with pings, and as this service is not needed to make networking work, many administrators have disabled the service.

> But what effect would it have if you just target one specific machine, if any?

Waste of bandwidth. When microsoft first invented networking 13 years after everyone else, they did a shoddy job as usual. There was a problem called the "Ping of Death", where sending an oversized ping would crash a windoze box. Every klown in the world thought this was great sport, until microsoft finally fixed the problem about 4 years later.

Old guy
.