

Re: TR: Mapping Class A network (any easy trick?)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0100.html>

From: James Riden (j.riden_at_massey.ac.nz)

Date: 02/22/05

To: Vicente Feito <vicente.feito@gmail.com>

Date: Tue, 22 Feb 2005 16:05:00 +1300

Vicente Feito <vicente.feito@gmail.com> writes:

> *I keep reading the same mistake over and over, not talking about this particular message, but about something most admins do, they start flooding the network with nmap and trying to do a broadcast scan, that's insane, they do nmap -sS -p1-65535 x.x.x.x/24 or something like that, I don't mean to criticize, but I'm my opinion, what I do if I need something like this, is first, just find out what hosts are up, something like nmap -sP <whatever>*

I believe that nmap does ping before doing the SYN scan by default, so it won't generate thousands of SYNs for hosts which aren't up.

-P0 Do not try to ping hosts at all before scanning them.

[snip]

By default, Nmap sends an ICMP echo request and a TCP ACK packet to port 80.

--

James Riden / j.riden@massey.ac.nz / Systems Security Engineer
GPG public key available at: <http://www.massey.ac.nz/~jriden/>
This post does not necessarily represent the views of my employer.