

RE: TFTP Scanner recommendation requested

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-08/0078.html>

From: Michael Gorsuch (mgorsuch_at_aikinetworks.com)

Date: 08/13/03

To: "'Barry Fitzgerald'" <bkfsec@sdf.lonestar.org>, <pen-test@securityfocus.com>
Date: Wed, 13 Aug 2003 16:26:50 -0500

The first place I would start is NMAP – if any machine responds with that port open, it needs to be checked regardless if there is an operating tftp server or not.

Hope this helps,

Michael Gorsuch
Aiki Network Security and Solutions
mgorsuch@aikinetworks.com
<http://www.aikinetworks.com>

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

From: Barry Fitzgerald [<mailto:bkfsec@sdf.lonestar.org>]
Sent: Wednesday, August 13, 2003 1:54 PM
To: pen-test@securityfocus.com
Subject: TFTP Scanner recommendation requested

Hello,

First of all, my office just got completely pelted with a scan looking for open udp/69 ports with tftp requests being made on each port. (Our IDS alerted me to this). I know that msblast opens up that port during the worm-infection period. So, the fact that this is happening right now is not surprising. Is anyone else noticing this? (I

know that we aren't infected with msblast, so it's not worm traffic – and I have verified that this is an automated backdoor scan.)

Anyway, the reason I'm writing this to the pen-test list is for a recommendation. I'd like to keep my eye out for open tftp servers on my LAN just in case. Does anyone have a recommendation for a tftp scanner that can scan a range of IPs for functioning tftp listeners?

This is for professional defense and pen testing, obviously, and not for a "how do I hack?" kind of BS request. :)

RE: TFTP Scanner recommendation requested

SecurityFocus Penetration: RE: TFTP Scanner recommendation requested

-Barry

