

IP-PBX, Easy Tests To Do (Ports)

[PRINT](#)

March 04, 2007

By Matt Brunk

Testing your IP-PBX doesn't mean exhausting your budget for the year.

Instead, no cost and low cost alternatives may help give you an edge. Any advantage in IP telephony is better than none. You will invest time and a lot of it. More time spent on the front-end (pre-cutover) means less time spent on the back-end (post-cutover). It's a simple equation.



ScanFi is a tool to scan your network from the inside going outward looking for open ports and vulnerabilities. It is FREE for a 30 day trial period. For more information on ScanFi:

Email: support@scanfi.com

Telephone: 1-888-720-9500

Web: <http://www.adventnet.com>

We placed a recently de-installed IP-PBX on one of our VLANs in our office and scanned only the box (IP-PBX). Here's just a small sampling of what ScanFi found:

CVEID: CAN-2000-0284

Type: Gain Admin Access

Bugtrack ID: 1110

Threat: Vulnerabilities have been found in COPY,LSUB,RENAME and FIND commands that could allow any attacker with a valid username/password combination to gain command shell access to the server where IMAPD is answering requests.

Solution: Upgrading to the latest version of IMAP will correct this as well as other vulnerabilities found in IMAP.

Reference: <http://www.washington.edu/imap/>

CVEID: CAN-1999-0619

Type: OpenPorts

Threat: The Telnet service is running in the remote host. The data between telnet client and server are transmitted in clear text and are not encrypted.

Open Ports:

Port	Protocol	Service
21	TCP	ftp
80	TCP	http
143	TCP	imap
4321	TCP	rwhois
111	UDP	rpcbind

Comment on this Article

[Click here to comment... \(Show/Hide Form\)](#)

Other Visitors Comments

There are no comments currently...

[Close Window](#)