

## RE: Using IPaqs or other handhelds as penetration devices

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-05/0065.html>

---

**From:** Eric Smith ([esmith@e-fense.com](mailto:esmith@e-fense.com))

**Date:** 05/16/02

From: "Eric Smith" <[esmith@e-fense.com](mailto:esmith@e-fense.com)>

To: <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Date: Thu, 16 May 2002 13:47:07 -0600

There are some tools that you could use to exploit wireless networks via the Compaq Ipaq PDA. Mini-Stumbler (downloadable from [www.netstumbler.com](http://www.netstumbler.com)) allows for wireless network reconnaissance. Essentially, through the use of a PCMCIA adapter for the IPAQ, you can use a standard 802.11b PCMCIA network card to find 802.11b wireless networks. Of course, once you're able to find these networks and determine the safeguards that are or aren't in place, you may be able to further penetrate the wired network easily without any further tools. There is also a similar \*nix version that can be used on the IPAQ (my memory fails me on the name right now), and it essentially does the same thing. A company named AirMagnet, Inc. ([www.airmagnet.com](http://www.airmagnet.com)) recently released a new version of their wireless vulnerability assessment tool (AirMagnet 1.2) that analyzes wireless networks through the use of a Compaq IPAQ and an 802.11b card. IMHO, extremely expensive tool considering you can get essentially the same tools for free from places like netstumbler and a bunch of other sites. There are some war-dialers (TBA - Palm war dialer from l0pht (now @stake)/ToneLoc Palm Edition 1.0 - not sure if either are still available.) and port scanners that have been released for systems with the Palm OS , but I haven't heard of any for the IPAQ. Maybe someone else could enlighten us on anything available in that realm for wired networks.

Eric Smith

Eric Smith, Computer Security and Investigations Specialist

e-fense, Inc. ([www.e-fense.com](http://www.e-fense.com))

6767 S. Spruce St., Ste. 215-S

Englewood, CO 80112

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

From: Johann van Duyn [[mailto:Johann\\_van\\_Duyn@bat.com](mailto:Johann_van_Duyn@bat.com)]

Sent: Thursday, May 16, 2002 03:19

To: [pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)

Subject: Using IPaqs or other handhelds as penetration devices

SecurityFocus Penetration: RE: Using IPaqs or other handhelds as penetration devices

Hi there...

I was wondering whether any exploits or penetration tools exist that run on Compaq IPaq PDAs (running Windows CE or whatever they call it now), or any other handheld devices, for that matter. This is part risk analysis regarding the use of such devices, and part looking at using such a device for lightweight ad-hoc penetration or vulnerability testing.

Thanks!

---

Johann van Duyn, CISSP  
IT Risk and Security Manager: British American Tobacco South Africa  
Stellenbosch, South Africa Tel. +27 (21) 8883765 Cel. +27 (82) 4588472  
Fax. +27 (21) 8838692  
E:mail: [johann\\_van\\_duyn@bat.com](mailto:johann_van_duyn@bat.com)

---

"... this leads you to assume that organization is an inherent property of the knowledge itself, and that disorder and chaos are simply irrelevant forces that threaten it from outside.

In fact it's exactly the opposite.

Order is simply a thin, perilous condition we try to impose on the basic reality of chaos..."

—William Gaddis, JR

Confidentiality Notice: The information in this document and attachments is confidential and may also be legally privileged. It is intended only for the use of the named recipient. Internet communications are not secure and therefore British American Tobacco does not accept legal responsibility for the contents of this message. If you are not the intended recipient, please notify us immediately and then delete this document. Do not disclose the contents of this document to any other person, nor take any copies. Violation of this notice may be unlawful.

---

-----  
This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

RE: Using IPaqs or other handhelds as penetration devices

- ***Previous message:*** William Knowles: "Re: Using IPaqs or other handhelds as penetration devices"
- ***In reply to:*** Johann van Duyn: "Using IPaqs or other handhelds as penetration devices"
- ***Next in thread:*** Peter Akre: "Re: Using IPaqs or other handhelds as penetration devices"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]