

Re: testing wireless security

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-11/msg00006.html>

- *From:* "Mark D. Foster" <mark@xxxxxxxx>
 - *Date:* Mon, 19 Nov 2007 15:55:07 -0800
-

Josh Paetzel wrote:

When I looked in to this it seemed that the current state of affairs is that WPA can only be broken by brute-forcing the key. I don't recall if that could be done 'off-line' or not. My memory is that the needed info to attempt bruteforcing could be done by simply receiving....no need to attempt to associate to the AP was needed. I'm not really interested in disseminating links to tools that can be used to break wireless security, but simple google searches will give you the info you need.....and the tools are in the ports tree for the most part.

Fortunately WPA allows keys that put even resource-rich attackers in to the decade range to bruteforce.

That would not appear to be a limitation of aircrack-ng
<http://www.freshports.org/net-mgmt/aircrack-ng/>

aircrack is an 802.11 WEP and WPA-PSK keys cracking program that can recover this keys once enough encrypted packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, thus making the attack much faster compared to other WEP cracking tools. In fact aircrack is a set of tools for auditing wireless networks.

That said, I haven't (yet) tried it myself ;)

—
Said one park ranger, 'There is considerable overlap between the intelligence of the smartest bears and the dumbest tourists.'
Mark D. Foster, CISSP <mark@xxxxxxxx> <http://mark.foster.cc/>

freebsd-security@xxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"