

## RE: V/Scan for Wireless LANs

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-07/0154.html>

---

**From:** Bartholomew, Brian J (*BartholomewBJ\_at\_state.gov*)

**Date:** 07/21/03

To: "'Ian Chilvers'" <Ian.Chilvers@prolateral.com>, "'pen-test@securityfocus.com'" <pen-test@secu  
Date: Mon, 21 Jul 2003 10:47:52 -0400

I have successfully cracked 40 and 104 bit WEP keys with reinj.c and Aircrack-ng or Kismet. Just use Aircrack-ng or Kismet to listen and store the "interesting" traffic, and reinj.c to create it. One usually needs between 100 MB to 1 GB of traffic to crack the key, but once the data is captured, the key cracks in a matter of seconds.

There is a good paper that describes the weak implementation of initialization vectors entitled "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin, and Adi Shamir. I suggest reading it.

I mentioned Kismet above. It is one of the best tools out there for WLAN testing. It allows you to perform a variety of things to the AP such as spoofing, disassociations, capture traffic, sniff out "hidden" APs, etc. It is all around a better tool to use than NetStumbler since it detects APs passively, instead of broadcasting everywhere. It even detects other NetStumbler clients.

The suggestion to brute force the key is not a good idea since, as one person already pointed out, it would take a very long time to BF it. It could be done I guess, but by the time the key is cracked, they would have probably already changed it.

Personally I think the best way of attack is to use some sort of man in the middle attack. If you are able to disassociate the clients from that AP and have them re-associate with you, you are golden :).

Brian J. Bartholomew  
U.S. Dept of State, Bureau of Diplomatic Security  
Computer Incident Response Team  
(202)663-2304

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

From: Ian Chilvers [mailto:Ian.Chilvers@prolateral.com]  
Sent: Friday, July 18, 2003 12:45 PM  
To: pen-test@securityfocus.com

SecurityFocus Penetration: RE: V/Scan for Wireless LANs

Subject: V/Scan for Wireless LANs

Hi all

We've been asked to perform a vulnerability assessment for a company that has a Wireless LAN. The W/LAN is running WEP with a random key generated, rather than a dictionary word.

Are there any tools out there that can brute force a WEP.

Take this example. A person parks the car in the car park and sniffs the air waves with a product like NetStumbler. He discovers the W/LAN but with WEP.

Is there a tool he can use to discover the WEP key (possible by brute force)

If there isn't such a tool, how does this sound for an idea.

Run a app that starts at binary 0's and counts upto 128bits of 1's  
For each sequence listen to see if there are any sensible packets or even send out a DHCP discover request to see if you get a reply. This would then possibly give you the WEP key.

Any comments

Ian....

---

KaVaDo is the first and only company that provides a complete and an integrated suite of Web application security products, allowing you to:

- assess your entire Web environment with a Scanner,
- automatically set positive security policies for real-time protection, and
- maintain such policies at the Application Firewall without compromising busines performance.

For more information on KaVaDo and to download a FREE white paper on Web applications – security policy automation, please visit:  
<http://www.kavado.com/ad.htm>

---

---