QUICK-FIX
COMPUTER SOLUTIONS

WEP [NETWORK SECURITY]

WEP	WPA	WPS

With clients	Without clients

Introduction :

This guide was created to demonstrate the encryption vulnerabilities of WEP (Wired Equivalent Privacy).

Breaking into a protected wireless network is illegal!
The content and instructions contained herein are for educational purposes, only. I did not break the law when creating this example. All information in the screenshots is that of my own networks that I compromised for this demonstration. You may attempt the steps outlined at your own risk - on your own network. If you wish to hack an other wireless network you must get permission from the network owner.

Breaking a WEP key involves using network monitoring software to capture weak IVs (initialization vectors) and a cracking software to decrypt them. The software we will be using in this guide is the aircrack-ng suite that is included with Backtrack linux.
There are several flavors of linux that come with this software including Auditor, Backtrack, and Kali linux.
In this guide we will be using Backtrack 5 R3.

Generally, the idea is to use your wireless adapter to capture any weak IVs being sent to/from the Access Point.
We capture these IVs by intercepting and relaying ARP requests to the Access Point causing it to reply with more IVs.
Once enough data (IVs) has been collected it can be decrypted using the Aircrack-ng software to display the wep key in plain text.

This guide has been divided into 2 sections as there are 2 possible scenarios that may be encountered when breaking a WEP key - each requiring a slightly different approach.

1) Capturing IVs with a client connected

2) Capturing IVs with no clients connected

Please read the following before continuing.....

The following is a direct Excerpt from Wikipedia :

Encryption details

WEP was included as the privacy of the original IEEE 802.11 standard ratified in September 1999.[5] WEP uses the stream cipher RC4 for confidentiality,[6] and the CRC-32 checksum for integrity.[7] It was deprecated as a wireless privacy mechanism in 2004, but for legacy purposes is still documented in the current standard.[8]

Basic WEP encryption: RC4 keystream XORed with plaintextStandard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. At the time that the original WEP standard was being drafted, U.S. Government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).

A 128-bit WEP key is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F). Each character represents 4 bits of the key. 4 × 26 = 104 bits; adding the 24-bit IV brings us what we call a "128-bit WEP key". A 256-bit WEP system is available from some vendors, and as with the above-mentioned system, 24 bits of that is for the I.V., leaving 232 actual bits for protection. This is typically entered as 58 Hexadecimal characters. (58 × 4 = 232 bits) + 24 I.V. bits = 256 bits of WEP protection.

Key size is not the only major security limitation in WEP.[9] Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic. There are other weaknesses in WEP, including the possibility of IV collisions and altered packets,[6] that are not helped at all by a longer key.

Authentication

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

For the sake of clarity, we discuss WEP authentication in the Infrastructure mode (ie, between a WLAN client and an Access Point), but the discussion applies to the Ad-Hoc mode too.

In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Thus, any client, regardless of its WEP keys, can authenticate itself with the Access Point and then attempt to associate. In effect, no authentication (in the true sense of the term) occurs. After the authentication and association, WEP can be used for encrypting the data frames. At this point, the client needs to have the right keys.

In Shared Key authentication, WEP is used for authentication. A four-way challenge-response handshake is used:

I) The client station sends an authentication request to the Access Point.
II) The Access Point sends back a clear-text challenge.
III) The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request.
IV) The Access Point decrypts the material, and compares it with the clear-text it had sent. Depending on the success of this comparison, the Access Point sends back a positive or negative response. After the authentication and association, WEP can be used for encrypting the data frames.